Fidelity National Financial, Inc
601 Riverside Avenue, Bldg. 5
Jacksonville, FL 32204
Tel 904.854.8954 Fax 904.633.3057

Elizabeth P. Reilly, Esq., CIPP/US
Compliance and Regulatory Counsel
elizabeth.reilly@fnf.com

FIDELITY NATIONAL FINANCIAL

May 4, 2017

VIA FEDERAL EXPRESS

Office of the Attorney General of the State of New Hampshire
33 Capitol Street
Concord, NH 03301

Re: Security Incident Notification

Dear Attorney General Foster,

Fidelity National Financial, Inc. ("FNF") is writing to inform you of an incident at one of our service providers that may have involved the personal information of approximately one New Hampshire resident. FNF's investigation into this incident is ongoing. The information provided below is based on our investigation findings to date.

On or about March 2, 2017, FNF learned that the Internal Revenue Service ("IRS") had recently sent letters to several FNF employees to alert them to potentially fraudulent tax returns filed in their names. In their discussions with the IRS, the employees learned that the fraudulent tax return filings contained accurate income information, leading the IRS to conclude that the employee's W-2 may have been obtained by the third-party fraudster.

Upon receiving this information, FNF promptly commenced an investigation in coordination with our tax service vendor, Ceridian Corporation. Our investigation included, among other things, analyzing log data from Ceridian's online W-2 portal, which provides FNF employees with access to their W-2s. Beginning on or about March 6, 2017, our log analysis determined that an unauthorized third party ("fraudster") created fraudulent accounts to the Ceridian portal for a limited number of FNF employees between January 11, 2017, and February 23, 2017. In addition to the confirmed fraudulent accounts, our log analysis also identified certain employee accounts that had been created using anomalous login credentials (*e.g.*, non-FNF email addresses) during the same time period. FNF was unable to verify whether these accounts were fraudulent based solely on the available log data, so we contacted these employees for additional information as part of our ongoing investigation. In total, our investigation has determined that the fraudster created unauthorized accounts to the Ceridian portal for 236 FNF employees.

Ceridian has advised FNF that the fraudster used legitimate personal information to create the unauthorized accounts to the Ceridian portal and that such information would have included the employee's name, zip code, and Social Security Number. FNF does not know where the fraudster obtained this information. To date, FNF has not identified any evidence suggesting that the information came from a breach of FNF systems. Ceridian has advised FNF that it similarly has not identified evidence indicating that the information came from a breach of its systems.

In response to the incident, Ceridian disabled FNF employee access to the online portal on March 3, 2017, and further disabled the ability for users to create new online accounts to the portal on March 4, 2017, both of which

currently remain disabled. FNF also notified the IRS and has been cooperating in its investigation. The IRS has advised FNF that it intends to refer the incident to the Federal Bureau of Investigation.

Based on our findings to date, FNF and Ceridian have determined that fraudulent online accounts were created for one New Hampshire resident. FNF has communicated with potentially impacted employees multiple times during our investigation, including to request additional information related to the investigation and, once a Ceridian portal account was determined to be fraudulent, to notify the impacted employee and offer identity theft services, as described below. Our first communication related to the incident was provided on March 8, 2017, a second communication was provided on April 7, 2017, and we plan to send a third communication on or about May 4, 2017. Additionally, potentially impacted employees were able to obtain additional information and communicate with FNF regarding their concerns either directly or through a call center the Company established in connection with the incident.

FNF is committed to helping its employees combat identity theft and fraud. We have partnered with Experian Consumer Direct to provide impacted employees with a free one-year membership to Experian Consumer Direct's CreditCheck Basic. FNF has also arranged for employees to utilize Equifax's ID Restoration service, which provides assistance and guidance for victims of identity theft to help restore identity as quickly and effectively as possible. In addition, our notification letter includes information to enable employees to protect themselves from identity theft, including information for the three national credit reporting agencies and the Federal Trade Commission, as well as information on how to obtain a credit report and how to put in place a fraud alert or credit freeze. The letter also includes recommendations to monitor accounts, and advice to report suspected identity theft to local law enforcement, the Attorney General, and/or the FTC. A copy of the notice letter is enclosed.

If you have any questions or concerns about this incident, please contact me at (904) 854-8954.

Sincerely,

Elizabeth P. Reilly
Compliance and Regulatory Counsel
Fidelity National Financial, Inc.

Encl.

Fidelity National Financial, Inc
601 Riverside Avenue, Bldg. 5
Jacksonville, FL 32204
Tel 904.854.8954 Fax 904.633.3057

Elizabeth P. Reilly, Esq., CIPP/US
Compliance and Regulatory Counsel
elizabeth.reilly@fnf.com

FIDELITY NATIONAL FINANCIAL

May 4, 2017

[Name]
[Address]
[City, State Zip]

Notice of Data Breach

Dear [Name],

Fidelity National Financial, Inc. ("FNF" or the "Company") recently communicated with you regarding an incident that may have impacted your personal information. We are sending you this follow-up letter regarding the same incident to provide you with additional information. The information below is based on our investigation to date.

What Happened

On or about March 2, 2017, FNF learned that the IRS had recently sent letters to several FNF employees to alert them to potentially fraudulent tax returns filed in their names. In their discussions with the IRS, the employees learned that the fraudulent tax return filings contained accurate income information, leading the IRS to conclude that the employee's W-2 was obtained by the third-party fraudster.

As our previous notice indicated, the Company promptly began investigating these reports. A step in that investigation was the review of our tax service vendor Ceridian's online W-2 portal and all user accounts created to access Company employee W-2s on that portal. Based on that review, we have reason to believe that the fraudster created several online accounts with the tax service vendor between January 11, 2017, and February 23, 2017. Our investigation indicates that one of these online accounts may have provided the fraudster with access to your W-2. We do not know whether a copy of your W-2 was obtained by an unauthorized person or whether your W-2 has been used in an attempt to file a fraudulent tax return. We do know that the creator of that online account had your Social Security Number, in addition to your name, zip code and the Company's vendor code, to create the account. Based on our investigation to date, we do not have evidence to suggest the fraudster obtained this information from FNF.

What Information Was Involved

As a result of this incident, the information in your W-2, including your Social Security Number, may be at risk.

What We Are Doing

The Company continues to work with Ceridian to investigate the incident. In response to the incident, Ceridian disabled FNF employee access to the online portal on March 3, 2017, and further disabled the ability for users to create new online accounts to the portal on March 4, 2017. The online access remains disabled. The FNF vendor code has also been changed.

FNF is committed to helping its employees combat identity theft and mortgage fraud. As mentioned in our prior communication to you, we have partnered with Experian Consumer Direct to provide you with a free one-year membership to Experian Consumer Direct's CreditCheck Basic. If you have not registered for this service yet and would like to do so, please contact experian@fnf.com.

You may also utilize Equifax's ID Restoration services. This service provides assistance and guidance for victims of identity theft to help restore identity as quickly and effectively as possible. For assistance, please call 877-368-4940.

What You Can Do

We recommend that you remain vigilant for fraud and identity theft. We have provided information in the enclosure regarding steps you can take to protect yourself against identity theft and potential misuse of your personal information.

Additionally, if you have received a LTR 4883 letter from the IRS or have received any other communication from the IRS this year asking for verification of identity or alerting to possible tax fraud, and you would like to let us know, please contact securityresponse@fnf.com.

For More Information

If you have any questions or concerns about this incident, please contact our response team at 855-474-3893 or email securityresponse@fnf.com.

Our investigation into this matter continues, and we will update you with any information we learn that may be helpful to you. We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

Elizabeth P. Reilly

Information about Identity Theft Prevention

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax, P.O. Box 105139, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian, P.O. Box 2002, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion, P.O. Box 6790, Fullerton, CA 92834-6790, 1-800-916-8800, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

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

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

For residents of Oregon: You are encouraged to report any suspected identity theft to the Oregon Attorney General.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-800-525-6285, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, www.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion, LLC, P.O. Box 2000, Chester, PA, 19022-2000, www.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion, LLC, P.O. Box 2000, Chester, PA, 19022-2000, www.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle

initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.