FIS»

FIDELITY NATIONAL
INFORMATION SERVICES

September 24, 2007

Ms. Lauren J. Noether
Bureau Chief
Consumer Protection & Anti-Trust
33 Capitol Street
Concord, NH 03301

RE: Fidelity National Information Services, Inc.
601 Riverside Avenue
Jacksonville, FL 32204

RE: Fidelity National Financial, Inc.
601 Riverside Avenue
Jacksonville, Fl 32204

Dear Ms. Noether:

Fidelity National Information Services, Inc. ("FIS"), for itself and on behalf of its customer Fidelity National Financial Inc. ("FNF"), is notifying the Department of Consumer Protection & Anti-Trust that an employee of FIS was the victim of the theft of a laptop computer containing nonpublic information regarding the employees of FIS and FNF. The theft of the laptop occurred in Jacksonville, Florida and a report of the theft was filed with the Jacksonville Police Department.

At this time, we have determined that there are thirty seven (37) New Hampshire residents affected, twenty nine (29) of which are employees of FIS and eight (8) of which are employees of FNF. Attached is a copy of the forms of notice which will be provided to those residents. We will begin mailing notices on September 24, 2007 and those notices will be mailed on or prior to September 27, 2007.

FIS is continuing its investigation and is in the process of resolving incorrect or incomplete addresses. If, as a result of that process, the number of affected New Hampshire residents' changes significantly, we will provide you with revised numbers.

Should you have any questions, please contact my office at 904-357-1663.

Sincerely

Fara E. Faubus

Fara Faubus
Chief Compliance Officer
Fidelity National Information Services, Inc.

FIS

FIDELITY NATIONAL INFORMATION SERVICES

September 24, 2007

[Insert Name]
[Insert Address]

Re: Important Notice Regarding Your Personal Information

Dear [Name]:

A laptop computer was recently stolen from an employee of Fidelity National Information Services, Inc. ("FIS"). This employee was providing technical assistance for the company's migration of payroll and human resource information to the Oracle system. Upon learning of the theft, FIS researched the information that was stored on the stolen laptop. That research revealed that the computer contained information from FIS' human resources database. You are receiving this letter because your name and social security number and, in some cases, additional personal information (such as employee number, address, email address, certain payroll information and/or date of birth) was contained on the stolen laptop. You can find out specifically what additional personal information of yours was on the laptop by contacting FTSHelpdesk@fnf.com or calling (866) 909-4569.

The laptop was password protected, and we have no reason to believe that your data has been compromised or utilized in an unauthorized manner. However, we have partnered with ConsumerInfo.com, Inc., an Experian® company, to provide you with a full year of credit monitoring. If you are concerned about the possibility of misuse, we encourage you to take advantage of this complimentary membership to Experian's Triple Alert℠. Features of this membership include daily monitoring of all three credit bureaus, e-mail alerts that inform you of key changes to your credit activity, and $10,000 of identity theft insurance coverage provided by Virginia Surety Company, Inc. (Due to New York state law restrictions, this coverage cannot be offered to residents of New York.). If you would like to take advantage of this offer, please enroll using the link and activation code appearing below:

http://partner.consumerinfo.com/fisemployee
[Activation Code]

Although we believe this theft does not present a significant risk to your identity, we strongly recommend that you remain vigilant and review your account statements carefully. If you notice any unauthorized activity, promptly contact your financial institution. Reviewing your credit report on a regular basis can also help you identify suspicious activity. On the reverse side of this letter is a Reference Guide that gives you more information on identity theft, how to report it and how to protect yourself from it.

FIS is a conscientious company that takes its responsibility to protect and preserve employee information very seriously. We deeply regret this unfortunate event and apologize for any inconvenience it has caused.

Sincerely,

Fred Parvey
Executive Vice President and
Chief Information Officer

REFERENCE GUIDE

Identity theft, in its simplest form, occurs when someone obtains and misuses your personal information without your permission, and often times without any knowledge of the activity by you. It is prudent to know about identity theft and what steps you can take to minimize your risk of potential identity theft or fraud. We recommend that you remain vigilant by reviewing account statements and monitoring free credit reports for the next twenty (24) months.

Free Fraud Alert. A fraud alert instructs creditors to watch for unusual or suspicious activity in your accounts, and provides creditors with notice to contact you separately before approving an extension of credit. To place a fraud alert, **free of charge**, contact one of the three national credit-reporting agencies listed below. You do not need to contact all three agencies; rather, the agency that you contact will forward the fraud alert to the other two agencies on your behalf. An initial fraud alert stays on your credit report for 90 days.

Equifax
Office of Fraud Assistance
P.O. Box 105069
Atlanta, GA 30348
(888) 766-0008
TTY: (866) 478-0030
http://www.equifax.com

Experian
Credit Fraud Center
P.O. Box 9532
Allen, TX 75013
(888) 397-3742
TTY: (800) 735-2989
http://www.experian.com

TransUnion
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834
(800) 680-7289
TTY: (877) 533-7803
http://www.tuc.com

Free Credit Report. Placing a fraud alert with each of the three consumer reporting agencies will also entitle you to a free credit report. When you place this alert, you will receive information about ordering a free credit report from each of the agencies. (If you elect not to place a fraud alert on your consumer credit file, you may still receive a free credit report by visiting www.annualcreditreport.com or calling toll-free (877) 322-8228.) We encourage you to obtain a free credit report, and to verify that any personal information listed is accurate.

Review Your Credit Report. Once you receive your reports, you should review them carefully for unusual credit activities, such as inquiries from companies you did not contact, accounts you did not open, and debts on your accounts that you cannot explain. You should verify the accuracy of your Social Security number, address(es), complete name and employer(s). If your credit report shows suspicious activity or unusual credit inquiries, you should immediately notify the agency that issued the report. You may also contact your local police or sheriff's office to file a report of identity theft. Be certain to obtain a copy of the police report. You may need to provide the police report to creditors in order to address any credit problems that may arise. We recommend that you check your credit reports and review your account statements periodically. This can help you spot problems and address them quickly.

Credit Freeze. Depending on the state that you live in, you may be eligible to place a security freeze on your consumer credit file with each of the three national credit bureaus. A security freeze prohibits credit agencies from sharing your credit file with any potential creditors without your consent. Once your files are frozen, even someone who has your personal information should not be able to obtain credit in your name. More information about security freezes is available through the websites of the three national credit reporting agencies — Equifax, Experian and TransUnion (website addresses are noted above).

Additional Information. Additional information about personal identity theft and fraud is available from the Federal Trade Commission ("FTC") at http://www.consumer.gov/idtheft. If you suspect identity theft, you may also file a complaint with the FTC at its website or by calling 1-877-ID-THEFT. Your complaint will be added to the FTC's Identify Theft Data Clearinghouse, where it will be accessible to law enforcement agencies for use in their investigations.

FIS

FIDELITY NATIONAL INFORMATION SERVICES

September 24, 2007

[Insert Name]
[Insert Address]

Re: Important Notice Regarding Your Personal Information

Dear [Name]:

As you may know, Fidelity National Information Services, Inc. ("FIS") provides certain technology-related services to Fidelity National Financial, Inc. ("FNF"), including payroll and human resource application hosting. Regrettably, a laptop computer was recently stolen from an FIS employee who was providing technical assistance for the database migration to the Oracle system. Upon learning of the theft, FIS researched the information being stored on the laptop. That research revealed that the computer contained information from FNF's human resources database. You are receiving this letter because your name and social security number and, in some cases, additional personal information (such as employee number, address, email address, certain payroll information and/or date of birth) was contained on the stolen laptop. You can find out specifically what additional personal information of yours was on the laptop by contacting FTSHelpdesk@fnf.com or calling (866) 909-4569.

The laptop was password protected, and we have no reason to believe that your data has been compromised or utilized in an unauthorized manner. However, we have partnered with ConsumerInfo.com, Inc., an Experian® company, to provide you with a full year of credit monitoring. If you are concerned about the possibility of misuse, we encourage you to take advantage of this complimentary membership to Experian's Triple Alert℠. Features of this membership include daily monitoring of all three credit bureaus, e-mail alerts that inform you of key changes to your credit activity, and $10,000 of identity theft insurance coverage provided by Virginia Surety Company, Inc. (Due to New York state law restrictions, this coverage cannot be offered to residents of New York.). If you would like to take advantage of this offer, please enroll using the link and activation code appearing below:

http://partner.consumerinfo.com/fisemployee
[Activation Code]

Although we believe this theft does not present a significant risk to your identity, we strongly recommend that you remain vigilant and review your account statements carefully. If you notice any unauthorized activity, promptly contact your financial institution. Reviewing your credit report on a regular basis can also help you identify suspicious activity. On the reverse side of this letter is a Reference Guide that gives you more information on identity theft, how to report it and how to protect yourself from it.

FNF and FIS are both conscientious companies that take their responsibility to protect and preserve your information very seriously. We deeply regret this unfortunate event and apologize for any inconvenience it has caused.

Sincerely,

Fred Parvey
Executive Vice President and
Chief Information Officer

REFERENCE GUIDE

Identity theft, in its simplest form, occurs when someone obtains and misuses your personal information without your permission, and often times without any knowledge of the activity by you. It is prudent to know about identity theft and what steps you can take to minimize your risk of potential identity theft or fraud. We recommend that you remain vigilant by reviewing account statements and monitoring free credit reports for the next twenty (24) months.

Free Fraud Alert. A fraud alert instructs creditors to watch for unusual or suspicious activity in your accounts, and provides creditors with notice to contact you separately before approving an extension of credit. To place a fraud alert, **free of charge**, contact one of the three national credit-reporting agencies listed below. You do not need to contact all three agencies; rather, the agency that you contact will forward the fraud alert to the other two agencies on your behalf. An initial fraud alert stays on your credit report for 90 days.

Equifax
Office of Fraud Assistance
P.O. Box 105069
Atlanta, GA 30348
(888) 766-0008
TTY: (866) 478-0030
http://www.equifax.com

Experian
Credit Fraud Center
P.O. Box 9532
Allen, TX 75013
(888) 397-3742
TTY: (800) 735-2989
http://www.experian.com

TransUnion
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834
(800) 680-7289
TTY: (877) 533-7803
http://www.tuc.com

Free Credit Report. Placing a fraud alert with each of the three consumer reporting agencies will also entitle you to a free credit report. When you place this alert, you will receive information about ordering a free credit report from each of the agencies. (If you elect not to place a fraud alert on your consumer credit file, you may still receive a free credit report by visiting www.annualcreditreport.com or calling toll-free (877) 322-8228.) We encourage you to obtain a free credit report, and to verify that any personal information listed is accurate.

Review Your Credit Report. Once you receive your reports, you should review them carefully for unusual credit activities, such as inquiries from companies you did not contact, accounts you did not open, and debts on your accounts that you cannot explain. You should verify the accuracy of your Social Security number, address(es), complete name and employer(s). If your credit report shows suspicious activity or unusual credit inquiries, you should immediately notify the agency that issued the report. You may also contact your local police or sheriff's office to file a report of identity theft. Be certain to obtain a copy of the police report. You may need to provide the police report to creditors in order to address any credit problems that may arise. We recommend that you check your credit reports and review your account statements periodically. This can help you spot problems and address them quickly.

Credit Freeze. Depending on the state that you live in, you may be eligible to place a security freeze on your consumer credit file with each of the three national credit bureaus. A security freeze prohibits credit agencies from sharing your credit file with any potential creditors without your consent. Once your files are frozen, even someone who has your personal information should not be able to obtain credit in your name. More information about security freezes is available through the websites of the three national credit reporting agencies — Equifax, Experian and TransUnion (website addresses are noted above).

Additional Information. Additional information about personal identity theft and fraud is available from the Federal Trade Commission ("FTC") at http://www.consumer.gov/idtheft. If you suspect identity theft, you may also file a complaint with the FTC at its website or by calling 1-877-ID-THEFT. Your complaint will be added to the FTC's Identify Theft Data Clearinghouse, where it will be accessible to law enforcement agencies for use in their investigations.