Re: Personal Information Security Notice

Dear_____,

As a valued employee, *Buyers Protection Group* (the "Company") writes to provide you with an important *notice* about the security of your personal information. In advance, the Company apologizes for any inconvenience that you may have experienced from the circumstances described below.

On July 19, 2015, a company laptop was stolen from an employee's car during a large-scale break in of at least 20 vehicles in the Greater Atlanta Area. The incident was immediately reported to the police and a police report was filed. Accordingly, we are working with local law enforcement and Fidelity National Financial's (parent company of BPG) security team to investigate the incident and take appropriate responsive action. In the course of FNF's security team investigation, it was discovered that a file containing your name, address, date of birth and social security number was likely on the laptop at the time of the theft.

Promptly after discovering this incident, we took action to discontinue login to BPG's online ordering system and redirected all users to Fidelity National Home Warranty's online ordering system. If the user's password on file for the BPG and FNHW website accounts was the same, the Company immediately disabled that password. As a result, you may be prompted to reset your password at your next visit to the FNHW online ordering system account. If you have visited the site recently, you may have already been asked to reset your password; if so, there is no further action required on your part. If you use the same username and password for other online accounts as you used for the BPG website, we recommend that you change those credentials as a precautionary measure.

In addition, the Company recommends that you consider taking the following steps to minimize your risk of potential identity theft or fraud.

Immediately Review Your Credit Report And Financial Accounts. Consumers who know or suspect that their personal information has been compromised should consider placing a fraud alert on their consumer credit file. 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 using any of the contact information listed below (including online by using the websites identified 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.

Equifax	**Experian**	**TransUnion**
(888) 766-0008	(888) 397-3742	(800) 680-7289
http://www.equifax.com	http://www.experian.com	http://fraud.transunion.com

Placement of a fraud alert will also entitle you to a free credit report from each of the three agencies. We encourage you to obtain free credit reports, and to verify that all of your private information listed on the reports (*e.g.,* home address, Social Security number) is accurate. You should also review these reports carefully for suspicious or unusual credit activities, such as accounts that you did not open or credit inquiries by companies with whom you do not recall applying for credit or a new credit account. In addition to reviewing your credit report, you should review your credit card and other financial accounts for any suspicious or unauthorized activity.

If your credit report or credit card or other financial accounts show suspicious or unauthorized activity, immediately notify the agency that issued the credit report, your credit card company, your bank and/or local law enforcement to file a report of identity theft. If you contact law enforcement, it is a good idea 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.

Credit Monitoring. Even if you do not discover any signs of suspicious or irregular activity on your credit reports, we recommend that you continue to check your credit reports, credit card and other financial accounts for any problems that may occur. Anyone who unlawfully accessed your private information may hold or share it with others for use at a later time.

Credit Freeze. You may want to consider placing a security freeze on your consumer credit file. 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 private information should not be able to obtain credit in your name. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each of the three national credit reporting agencies. The credit reporting agencies require that security freeze requests be made in writing or online using the information listed below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com/Freeze

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
http://freeze.transunion.com

Finally, information about personal identity theft and fraud may be obtained from the Federal Trade Commission at http://www.consumer.ftc.gov/ or by calling 1-877-FTC-HELP.

If you have further questions about this incident, please send an email to privacy@bpgwi.com and a Company representative will be able to address any questions you may have related to this matter. Again, we deeply regret any inconvenience or concern this incident may cause you.

Sincerely,

BPG Customer Care