



Oldcastle Law Group
900 Ashwood Parkway, Suite 600
Atlanta, GA 30338-4780
Tel: (770) 392-5333
Fax: (770) 392-5305

HEATHER E. HARPER
Deputy General Counsel

January 2, 2013

VIA FEDERAL EXPRESS

The Honorable Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: **Data Breach Notification**

Dear Attorney General Delaney:

Please be advised that on or about December 13, 2012, Oldcastle APG, Inc. ("Company") learned that an employee's laptop was stolen during a break-in to her car on or around December 10, 2012. We believe the laptop may have contained some personal information relating to APG employees, including but not limited to, names, bank account information and social security numbers. Immediately upon learning of the theft, the Company contacted the Dekalb County Georgia Sheriff's Department and a police report was filed. To date, the laptop has not been recovered.

It appears that as many as 5,083 individuals could have been affected, including 22 residents of New Hampshire. To date, the Company has received no information indicating this information has been improperly utilized. All potentially affected individuals will be notified in the next several days. A draft copy of the notification that will be sent is enclosed.

The company has taken numerous steps to protect the security of the personal information of the affected individuals. Also, in addition to continuing to monitor this situation, the company is reexamining its current data privacy and security policies and procedures to find ways of reducing the risk of future data breaches. Should the company become aware of any significant developments concerning this situation, we will inform you.

If you require any additional information on this matter, please call me.

Very truly yours,


Heather E. Harper

Enclosure



Oldcastle®
Architectural

Dear Oldcastle APG Employee,

We are writing to you because of a recent security incident at Oldcastle APG that we learned about on December 13, 2012. An employee's car was broken into and her laptop was stolen on or around December 10, 2012. We believe the laptop may have contained some personal information relating to APG employees, including but not limited to, names, bank account information and social security numbers.

Immediately upon discovering the theft, APG filed a report with the Dekalb County Sheriff's Office and an investigation is underway.

Based on the information available, APG believes that the theft of the laptop was solely for the value of the laptop, and we are aware of no specific intent to access employee data. We also are not aware of any improper access to or use of the personal information contained on the laptop. In addition, APG has activated various programs that will wipe all data from the computer should the machine be connected to the internet. However, in an excess of caution, we are sending this advisory to you and other individuals whose personal information may have been contained in the laptop to make you aware of this incident so that you can take steps to protect yourself and minimize the possibility of misuse of your information. The attached sheet describes several no-cost steps you can take to protect your identity, credit and personal information.

We apologize for this situation and any inconvenience it may cause you.

We treat all sensitive employee information in a confidential manner and are proactive in the careful handling of such information. We continue to assess and modify our privacy and data security policies and procedures to prevent similar situations from occurring.

If you have questions or concerns you should call Sue Furlough, Director of Shared Services, Oldcastle Architectural, Inc., at (678) 731-8173.

Sincerely,

Michael Schaeffer
Chief Financial Officer
Oldcastle Architectural, Inc.

**Architectural
Products Group**
Oldcastle, inc.
A CRH plc Company
900 Ashwood Parkway, Suite 600
Atlanta, Georgia 30338
TEL: 770-804-3363
FAX: 770-804-3369

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

What You Should Do to Protect Your Personal Information

We recommend you remain vigilant and consider taking one or more of the following steps to protect your Personal Information ("PI"):

1. Contacting the nationwide credit-reporting agencies as soon as possible to:
 - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
 - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
 - Receive a free copy of your credit report by going to www.annualcreditreport.com.

Equifax
P.O. Box 740256
Atlanta, GA 30374
(800) 525-6285
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
www.experian.com/consumer

TransUnion
P.O. Box 2000
Chester, PA 19022
(800) 888-4213
www.transunion.com

2. If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen PI before using it.
3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues and how to avoid identity theft. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local police and you also can report this to the Fraud Department of the FTC, who will collect all information and make it available to law-enforcement agencies. Contact information for the FTC is:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580

4. *For North Carolina Residents:* For more information on identity theft please contact either the Federal Trade Commission at the contact information provided above, or North Carolina's Attorney General's Office, Address: 9001 Mail Service Center, Raleigh, NC 27699-9001; Telephone: (919) 716-6400; Fax: (919) 716-6750; website: www.ncdoj.com/
5. *For Maryland Residents:* The contact information for the State's Office of the Attorney General, which provides information about how to avoid identity theft, is

Honorable Douglas F. Gansler
Office of the Attorney General
200 St. Paul Place

Website: <http://www.oag.state.md.us>
Telephone number: (888) 743-0023
(toll-free in Maryland)

Baltimore, MD 21202

6. *For Massachusetts Residents:* Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses above:

In order to request a security freeze, you will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security Number;
- Date of birth;
- If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
- Proof of current address such as a current utility bill or telephone bill;
- A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.)
- If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
- If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and

social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.