Kathryn P. Sherer
Assistant General Counsel and Assistant Secretary

1000 Stanley Drive, New Britain, CT 06053
T (860) 827 3973 F (860) 827 3911

April 15, 2013

Michael A. Delaney, Esq.
Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Dear Mr. Delaney:

On March 8, 2013, I provided you with a letter, on behalf of Stanley Black & Decker, Inc., regarding the theft of a Stanley laptop. A copy of that letter is attached.

In mid-March, we discovered that, due to a data merge error, the list we had compiled of potentially affected individuals, all of whom are current or former employees, had incorrect addresses for some, but not all, of those affected. In the course of our efforts to address this issue, we also discovered that the stolen laptop may have included the Social Security number for some, but not all, of those affected.

As a result, Stanley is currently preparing to send new notices to all affected individuals. In addition, although we have not received reports of any incidents that suggest that information on the laptop has been used, Stanley will be offering two years of identity theft protection services to all affected individuals at the Company's expense. Seven of those individuals are New Hampshire residents.

Enclosed is a copy of the notice we will be sending to the affected individuals within the next few days.

Please do not hesitate to contact me at (860) 827-3973 if you have any questions or concerns.

Sincerely,

Kathryn P. Sherer
Assistant General Counsel

Attachment

StanleyBlack&Decker

Kathryn P. Sherer
Assistant General Counsel and Assistant Secretary

1000 Stanley Drive, New Britain, CT 06053
T (860) 827 3973 F (860) 827 3911

March 8, 2013

Mr. Michael A. Delaney
Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Dear Mr. Delaney:

On behalf of Stanley Black & Decker, Inc., I am writing to inform you about a recent incident in which personal information relating to New Hampshire residents may have been accessed by an unauthorized third party.

Specifically, we recently learned that a company-issued laptop was stolen. Through our investigation, we have determined that the laptop contained information regarding certain of our employees, including, in some cases, an employee's name and the account number and routing number of the account that the employee has designated as the account into which reimbursements for corporate expenses should be deposited and from which any personal expenses charged to the company should be debited.

As a result, we will notify 5 employees who are New Hampshire residents of this theft. This notice will be mailed within the next few days. Please do not hesitate to contact me at (860) 827-3973 if you have any questions or concerns.

Sincerely,

Kathryn P. Sherer
Assistant General Counsel

dc-706844

[SBD LETTERHEAD]

April ___, 2013

Experian Activation Code: [redacted]

[Name]
[Address]

Dear **[Name]**:

In March, Stanley Black & Decker sent out notices to certain employees and former employees regarding the theft of an employee laptop that may have contained their personal information. Unfortunately, due to a data merge error, some of those notices may not have reached their intended recipients. In addition, during the course of our efforts to resolve the data merge issues, we determined that additional information may have been included in files on the laptop that was not reflected in the original notices.

More particularly, on January 28, 2013, the company-issued laptop of an employee in the Finance department who handled T&E charges was stolen. Through our investigation of the incident, we believe that information stored on the laptop may have included your name and the account number and routing number of the account that you have designated as the account to which direct deposits are to be made to reimburse you for expenses incurred on the Company's behalf. Information stored on the laptop may also have included your social security number.

We deeply regret that this incident occurred and take very seriously the security of personal information. We recommend that you closely monitor your bank statements for the relevant account to identify any suspicious or unusual activity on your account. If you discover any suspicious or unusual activity, you should immediately report it to your financial institution.

Due to the nature of the information involved, the Company is offering all potentially affected employees a two year membership in Experian's ProtectMyID Alert service at no expense to you. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Once your ProtectMyID membership is activated, your credit report will be monitored daily for 50 leading indicators of identity theft. You'll receive timely Credit Alerts from ProtectMyID on any key changes in your credit report which could include new inquiries, new credit accounts, medical collections and changes to public records. If identity theft is detected, ProtectMyID will assign a dedicated U.S.-based Identity Theft Resolution Agent who will walk you through the process of fraud resolution from start to finish for seamless service. As an added protection, you will receive Experian's ExtendCARE™ service, which provides you with the same high-level of Fraud Resolution support after your ProtectMyID membership has expired.

Should you wish to activate this service, go to the website, www.protectmyid.com/redeem or call 877-371-7902 and provide the Experian Activation Code included at the top of this letter **by July 31, 2013**.

Whether or not you activate this service, you should remain vigilant for identity theft and incidents of fraud, including by regularly reviewing your credit reports. You may contact the Federal Trade Commission ("FTC") or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's Web site, at

http://www.ftc.gov/idtheft/, call the FTC, at (877) IDTHEFT (438-4338), or write to, Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain your credit report from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(800) 525-6285	(888) 397-3742	(800) 680-7289
P.O. Box 740241	P.O. Box 9532	Fraud Victim Assistance Division
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 6790
www.equifax.com	www.experian.com	Fullerton, CA 92834-6790
		www.transunion.com.

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. In addition, you may also contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization.

Please know that we regret any inconvenience or concern this incident may cause you. Be assured that Stanley Black & Decker has safeguards in place to protect the security of employee information. Please do not hesitate to contact Tamara Candler, Director, North America Shared Services at 317-558-1640 or call us toll free at 877-795-2356 if you have any questions or concerns.

Sincerely,

Kristina Cerniglia
Corporate Controller

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission	Office of the Attorney General
Consumer Response Center	Consumer Protection Division
600 Pennsylvania Avenue, NW	200 St. Paul Place
Washington, DC 20580	Baltimore, MD 21202
(877) IDTHEFT (438-4338)	(888) 743-0023
http://www.ftc.gov/idtheft/	www.oag.state.md.us

IF YOU ARE AN IOWA RESIDENT: You may report suspected incidents of identity theft to the Iowa Attorney General. This office can be reached at:

Iowa Attorney General
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
http://www.iowaattorneygeneral.gov/

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

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

North Carolina Department of Justice
Attorney General Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.com