McLane, Graf,
Raulerson & Middleton
Professional Association

900 Elm Street | P.O. Box 326 | Manchester, NH 03105-0326
Tel: 603.625.6464 | Fax: 603.625.5650 | www.mclane.com

OFFICES IN:
MANCHESTER
CONCORD
PORTSMOUTH
WOBURN, MA

CAMERON G. SHILLING
Direct Dial: (603) 628-1351
Email: cameron.shilling@mclane.com
Licensed in NH and MA

February 11, 2013

Via U.S. Mail
Attorney General Michael A. Delaney
Office of the Attorney General
33 Capital Street
Concord, NH 03301

Re: Wallboard Supply Company - Data Breach Notification

Dear Attorney General Delaney:

The McLane law firm represents Agincourt Wallboard, LLC d/b/a Wallboard Supply Company ("Wallboard"), which is headquartered in Londonderry, New Hampshire. We are writing to inform you about a recent data security breach at Wallboard that affects 36 residents of New Hampshire.

On January 17, 2013, Wallboard learned that eight of its employees received a physical payroll check, rather than having their wages deposited directly into their bank accounts, as was the norm for them. Wallboard immediately launched an investigation into the matter, notified and filed a report with law enforcement, and gave notice to its employees orally and by email.

Wallboard learned from its payroll vendor that someone had used the administrator's credentials to access (without authorization) Wallboard's payroll system. The payroll system contained the names and addresses of Wallboard's sixty-two employees, their social security numbers, their bank account routing information, and other employment information about them. The payroll vendor also informed Wallboard that the hacker had change the bank account routing information for ten of its employees in an apparent attempt to route payroll payments to new accounts controlled by the hacker. Fortunately, due to safeguards built into the payroll system, the hacker was unable to effect any transfers of funds to the new bank accounts, and neither Wallboard nor any of its employees sustained any financial losses.

Wallboard believed at the time that the hacker also had attempted to use the bank account routing information to access the account of one employee. Wallboard has since learned that did not occur, and the company has no evidence to date that the hacker or anyone else has attempted to use the personal information of its employees to either access their accounts or engage in identity theft.

Since learning of the breach, Wallboard has been actively investigating how the hacker could have obtained the administrator's credentials, which consisted of an unique and strong password that was not written anywhere or shared with anyone. At present, Wallboard has not yet determined specifically

how the breach occurred, and is continuing an active investigation to determine the cause of the breach and implement remedial measures.

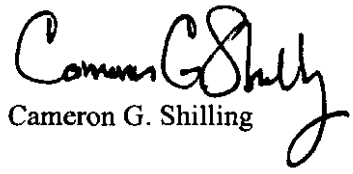
One possible cause of the breach is malware. Despite robust firewall, anti-malware and anti-virus protections on its network, Wallboard found that five of its computers were infected with a new Trojan horse, called Mal/JavaJar-B, which exploits a vulnerability in Oracle's Java 7. Wallboard does not yet know whether the presence of this malware enabled the hacker to obtain the administrator's credentials for its payroll system, and is following up on that matter with us and computer forensic experts. Wallboard also is following up with us, forensic experts, representatives of the banks involve, and law enforcement to investigate whether the hacker obtained the administrator's credentials through other means, and to potentially identify and catch the hacker.

Wallboard has implemented a number of remedial measure to protect its employees from this hacker and avoid potential future breaches. For example, Wallboard immediately changed the administrator's credentials; the payroll vendor installed new software that will enable it to better track unauthorized activities; and Wallboard created additional layers of security in the payroll system (e.g., requests to alter bank account information will trigger an automatic authorization and approval process, and if more than two changes are made from an administrator's account, a supplementary authorization and approval process will be required). Also, Wallboard's computer forensics experts removed the malware and installed new firewall protections, new anti-virus software, and additional anti-malware software. Wallboard will continue to implement additional remedial measure as it obtains further information about how this breach occurred.

On January 19, 2013, Wallboard notified all of its employees (including employees how are Vermont residents) about the breach both orally (by telephone or personally) and email. This preliminary notification informed the individuals about the facts of this breach and the type of personal information potentially compromised, and gave recommendations as to the type of immediate the individuals should take to protect themselves financially and their personal information. In addition to that preliminary notice, Wallboard provides the attached template of the written notice that was sent to all the affected New Hampshire residents consistent with New Hampshire law.

We trust that this letter provides you with all the information required to assess this incident and the adequacy of Wallboard's response. Please let us know if you have additional questions or if we can be of further assistance. I can be reached at the telephone number and email address provided.

Very truly yours,



Cameron G. Shilling

cc: Wallboard Supply Company

February 11, 2013

Via First Class Mail
New Hampshire Resident

On January 19, 2013, Wallboard gave employees notice about a security breach of its payroll system. In that notice, Wallboard described its understanding of the general nature of the situation and the type of information compromised, and gave some recommendations as to the immediate actions employees should have taken to protect themselves financially and their personal information. This notice now provides more comprehensive information about the incident.

On January 17, 2013, Wallboard learned that eight of its employees received a physical payroll check, rather than having their wages deposited directly into their bank accounts, as was the norm for them. Wallboard immediately launched an investigation into the matter, notified and filed a report with law enforcement, and gave notice to its employees orally and by email.

Wallboard learned from its payroll vendor that someone had used the administrator's credentials to access (without authorization) Wallboard's payroll system. The payroll system contained the names and addresses of Wallboard's employees, their social security numbers, their bank account routing information, and other employment information about them. The payroll vendor also informed Wallboard that the hacker had change the bank account routing information for 10 of its employees in an apparent attempt to route payroll payments to new accounts controlled by the hacker. Fortunately, due to safeguards built into the payroll system, the hacker was unable to effect any transfers of funds to the new bank accounts, and neither Wallboard nor any of its employees sustained any financial losses.

Wallboard believed at the time that the hacker also had attempted to use the bank account routing information to access the account of one employee. Wallboard has since learned that did not occur, and the company has no evidence to date that the hacker or anyone else has attempted to use the personal information of its employees to access their accounts or engage in identity theft.

Since learning of the breach, Wallboard has been actively investigating how the hacker could have obtained the administrator's credentials, which consisted of an unique and strong password that was not written anywhere or shared with anyone. At present, Wallboard has not yet determined specifically how the breach occurred, and is continuing an active investigation to determine the cause of the breach and implement remedial measures.

One possible cause of the breach is malware. Despite robust firewall, anti-malware and anti-virus protections on its network, Wallboard found that five of its computers were infected with a new Trojan horse, called Mal/JavaJar-B, which exploits a vulnerability in Oracle's Java 7. Wallboard does not yet know whether the presence of this malware enabled the hacker to obtain the administrator's credentials for its payroll system, and is following up on that matter with its attorneys and computer forensic experts. Wallboard also is following up with its attorneys, forensic experts, representatives of the banks involve, and law enforcement to investigate

whether the hacker obtained the administrator's credentials through other means, and to potentially identify and catch the hacker.

Wallboard has implemented a number of remedial measure to protect its employees from this hacker and avoid potential future breaches. For example, Wallboard immediately changed the administrator's credentials; the payroll vendor installed new software that will enable it to better track unauthorized activities; and Wallboard created additional layers of security in the payroll system. Also, Wallboard's computer forensics experts removed the malware and installed new firewall protections, new anti-virus software, and additional anti-malware software. Wallboard will continue to implement additional remedial measure as it obtains further information about how this breach occurred.

Wallboard reiterates that employees should take precautionary measures to protect their financial accounts and integrity of their personal information. If you have not already done so, as we recommended on January 19, 2013, we believe that you should contact (1) all your banks; (2) your credit card companies; and, (3) the three national credit reporting agencies. When you contact them you should inform them that your account may have been compromised, ask that they put a fraud alert on your account, and to check recent activity with your account for potentially fraudulent activity.

Here are the three phone numbers for the three national credit reporting agencies:

Equifax: 800-685-1111
TransUnion: 800-888-4213
Experian: 1-888-397-3742

We take this incident seriously and are committed to assure the security of your data. To help protect your identity, we are offering a complimentary one-year membership of Experian's ProtectMyID™ Elite. 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.

Activate ProtectMyID Now in Three Easy Steps

1. **ENSURE that you enroll by: May 31, 2013**
2. **VISIT www.protectmyid.com/enroll or call 877-441-6943 to enroll**
3. **PROVIDE your activation code: [code]**

Once your ProtectMyID membership is activated, your credit report will be monitored daily for 50 leading indicators of identity theft. You will receive timely Surveillance Alerts™ from ProtectMyID on any key changes in your credit report, a change of address, or if an Internet Scan detects that your information may have been found in an online forum where compromised credentials are traded or sold. ProtectMyID provides you with identity protection that will help detect, protect and resolve potential identity theft. In the case that 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.

Your complimentary 12-month ProtectMyID membership includes:

- **Credit Report:** A free copy of your Experian credit report
- **Surveillance Alerts**
  - **Daily 3 Bureau Credit Monitoring:** Alerts you of suspicious activity including new inquiries, newly opened accounts, delinquencies, or medical collections found on your Experian, Equifax, and TransUnion credit reports
  - **Internet Scan:** Alerts you if your Social Security Number or Credit and/or Debit Card numbers are found on sites where compromised data is found, traded or sold.
  - **Change of Address:** Alerts you of any changes in your mailing address.
- **Identity Theft Resolution:** If you have been a victim of identity theft, you will be assigned a dedicated, U.S.-based Experian Identity Theft Resolution Agent who will walk you through the fraud resolution process, from start to finish.
- **ExtendCARE:** Full access to the same personalized assistance from a highly-trained Fraud Resolution Agent even after your initial ProtectMyID membership expires.
- **Lost Wallet Protection:** If you ever misplace or have your wallet stolen, an agent will help you cancel your credit, debit and medical insurance cards.
- **$1 Million Identity Theft Insurance*:** As a ProtectMyID member, you are immediately covered by a $1 Million insurance policy that can help you cover certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-441-6943.

We apologize and know that this is a significant inconvenience. We are doing everything we can to work with law enforcement, information technology experts, and our lawyers to catch the hacker and remedy the situation. If there is anything we can do to assist you please call me at (603) 965-1104.

Sincerely,

Kerri Enwright
Director of Human Resources