

February 11, 2013

Via First Class Mail
Vermont 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. Below is a check list of suggestions of how employees can best protect themselves.

1. **Review your bank, credit card and debit card account statements** over the next twelve to twenty-four months and immediately report any suspicious activity to your bank or credit unions, or another financial institutions affected.

2. **Monitor your credit reports** with the major credit reporting agencies.

Equifax	Experian	TransUnion
1-800-685-1111	1-888-397-3742	1-800-916-8800
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

3. Under Vermont law, you are entitled to a free copy of your credit report from those agencies every twelve months. Get a credit report every 12 months.
4. Call the credit reporting agency at the telephone number on the report if you find:
 - Accounts you did not open.
 - Inquiries from creditors that you did not initiate.
 - Inaccurate personal information, such as home address and Social Security number.
5. If you do find suspicious activity on your credit reports or other account statements, call law enforcement and **file a report of identity theft**. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records, and also to access some services that are free to identity theft victims.
6. If you find suspicious activity on your credit reports or other accounts, **consider placing a fraud alert** on accounts and with the above agencies so creditors will contact you before opening new accounts. Call any one of the three credit reporting agencies at the number below to place fraud alerts with all of the agencies.

Equifax
888-766-0008

Experian
888-397-3742

TransUnion
800-680-7289

7. If you find suspicious activity on your credit reports or on your other account statements, consider placing a security freeze on your credit report so that the credit reporting agencies will not release information about your credit without your express authorization. A security freeze may cause delay should you wish to obtain credit and may cost some money to get or remove, but it does provide extra protection against an identity thief obtaining credit in your name without your knowledge. If you have Internet access and would like to learn more about how to place a security freeze on your credit report, please visit the Vermont Attorney General's website at:
<http://www.atg.state.vt.us/issues/consumer-protection/identity-theft.php>.

8. You may also get information about security freezes by contact the credit bureaus at the following internet addresses:

Equifax: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Experian: http://www.experian.com/consumer/security_freeze.html

TransUnion: <http://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/securityFreeze.page>

9. If you do not have Internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).
10. Even if you do not find suspicious activity on your credit report or your other account statements, it is important that you **check your credit report** for the next two years. Just call one of the numbers in paragraph 2 above to order your reports or to keep a fraud alert in place.
11. Helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report is available on the Vermont Attorney General's website at <http://www.atg.state.vt.us>.

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
Human Resources Manager