CRANE CO. 100 FIRST STAMFORD PLACE STAMFORD, CT 06902-6784

ANTHONY M. D'IORIO
DEPUTY GENERAL COUNSEL
AND ASSISTANT SECRETARY

Tel: (203) 363-7243
adiorio@craneco.com

June 8, 2016

Via U.S. Mail

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

I am writing on behalf of Crane Co. ("Crane") to inform you of a security incident potentially affecting fifteen (15) New Hampshire residents.

On June 7, 2016, an employee of Crane was targeted by an e-mail scam, called "spoofing." The spoofed e-mail appeared to come from a member of Crane's executive team and asked for employees' W-2 information. Because the recipient/employee wrongly believed the e-mail to contain a valid request from an executive, the employee replied by attaching the federal Form W-2 for the requested Crane employees. Crane immediately learned of the incident and began the steps necessary to provide notice and an identity protection product to affected individuals.

Crane sent a notification to all potentially affected New Hampshire residents on or about June 7, 2016. We will offer them a two-year membership in Experian's ProtectMyID Elite identity protection product at no cost to them. A copy of the template notice is enclosed with this letter.

If you have any questions concerning this matter, please do not hesitate to contact me.

Very truly yours,

Anthony M. D'Iorio
Deputy General Counsel

Enclosure

CRANE PAYMENT INNOVATIONS

June 7, 2016

[redacted]

Dear [redacted],

I am writing to inform you about a security incident involving your personal information and to let you know the steps that Crane Payment Innovations, Inc. ("CPI") is taking to address it.

Earlier today, a CPI employee responded to an e-mail that appeared to come from me, requesting a copy of your 2015 W-2 wage statement, which included your Social Security number, wage information and home address. Unfortunately, we learned later that day that the e-mail was not, in fact, from me, but rather was part of a fraudulent scheme, and your personal information was sent to an unknown individual.

CPI promptly contacted the FBI concerning this incident and will cooperate as required in their pursuit of the wrongdoer. As of this writing, CPI has received no information suggesting that your personal information has been misused.

Nonetheless, out of an abundance of caution, CPI is offering you two years of identity protection at no cost to you. Your two-year membership in Experian's ProtectMyID™ Elite product will help you to detect possible misuse of your personal information and will provide identity protection services focused on identification and resolution of possible identity theft. Once you activate your ProtectMyID Elite membership, your credit report will be monitored daily for 50 leading indicators of identity theft. You will receive timely credit alerts from ProtectMyID Elite on any key changes in your credit report. Your ProtectMyID membership also includes $1 million in identify theft insurance, which covers certain costs including private investigator fees, and unauthorized electronic fund transfers.

If you wish to enroll in ProtectMyID Elite, you will need to do the following:

1. **VISIT** The ProtectMyID Elite Web Site: **http://www.protectmyid.com/protect** or call 866-751-1324 to enroll
2. **PROVIDE** Your Activation Code: [redacted]

Enrollment Deadline: September 30, 2016

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions concerning Experian's ProtectMyID™ Elite or if you prefer to enroll over the phone for delivery of your membership via US mail, please call Experian at 866-751-1324.

In addition to arranging for two years of free credit monitoring, we have included with this letter additional information on steps you can take to protect the security of your personal information. We urge you to review this information carefully.

Please know that CPI takes the security of your personal information seriously, and we sincerely regret any inconvenience this incident might cause you. We encourage you to take advantage of the protections outlined in this letter. If you have any questions, please contact your local HR Business Partner by e-mail or telephone. Further information will be provided in upcoming meetings that are currently being arranged.

Sincerely,

Kurt Gallo
President, CPI

Crane Payment Innovations ("CPI" or the "Company") Security Incident
Frequently Asked Questions (FAQs)
FOR INTERNAL USE ONLY

Questions About The Incident

1. What happened?

On June 7th, CPI learned that an individual, whose identity is not known to the Company, fraudulently obtained certain personal information about CPI associates.

2. Can you give me more information about what happened? Was this a hack?

A CPI employee responded to an e-mail that appeared to come from CPI's President, requesting a copy of some associates' 2015 W-2 wage statements, which included Social Security numbers, wage information and home addresses. Unfortunately, we learned later that day that the e-mail was not, in fact, from the President, but rather was part of a fraudulent scheme, and that the personal information had been sent to an unknown individual.

3. What information did the individual obtain?

The individual obtained associates' personal information, including name, Social Security number, home address, and 2015 compensation data. Fortunately, the individual did not obtain any credit or debit card numbers.

4. Is my personal information at risk of being misused?

We have no information suggesting that your personal information has been misused. However, there is a risk that your information could be misused. We encourage you to activate the identity protection product described in the notice letter and to take the other steps described in that letter.

5. What is the earliest date at which suspicious activity might have occurred due to this incident?

The earliest date on which any suspicious activity could have occurred is June 7, 2016.

6. What is the Company doing about the situation?

Although we have no information to suggest that the personal information has been misused, CPI is providing two years of identity protection to all affected individuals. In addition, the Company has reported the incident to the FBI and will cooperate as required in their pursuit of the wrongdoer.

7. What is the total number of associates affected by this incident?

We can confirm that your personal information was affected, but we cannot comment on the impact of this incident on other associates.

8. What is the Company doing to ensure that this does not happen again?

We can assure you that the Company is taking this incident extremely seriously. We will be providing additional training to all relevant associates. We are also enhancing the Company's information security to further reduce risk in this area.

9. Have you contacted law enforcement?

Yes, we have contacted the FBI. We will cooperate fully with any investigation.

10. What should I do if I am contacted by the news media about this?

Follow the Company's standard media policy regarding statements to the media on the Company's behalf. Please refer any inquiries from the news media for comments on the Company's behalf to Jason Feldman, Director of Investor Relations, at 203-363-7329, jfeldman@craneco.com. Do not respond to any questions for the Company. Simply say: "Mr. Feldman will try to provide you with answers to your questions" and provide them with his contact details.

Questions About Services the Company Has Arranged

11. What is credit monitoring?

Monitoring your credit reports regularly is your first line of defense. Credit monitoring is a very effective tool for becoming aware of fraudulent activity. Every week, you'll be informed of changes to your credit report, alerting you to activities such as:

- New inquiries
- New accounts opened in your name
- Late payments
- Improvements in your report
- Bankruptcies and other public records
- New addresses

12. What type of credit monitoring service is the Company offering?

The Company is providing you with **two years of free credit monitoring** through Experian. This product is known as ProtectMyID® Elite.

13. What are the benefits of credit monitoring through ProtectMyID Elite?

Early detection is the key to identifying fraud and preventing the damage it can cause. Monitoring alerts make you aware of changes in your credit file that could indicate the kind of unauthorized activity commonly associated with identity theft and fraud.

ProtectMyID Elite monitors credit reports of individuals with established credit. The benefits include the following:

(a) Monitoring the Experian credit file every day and email alerts of key changes indicating possible fraudulent activity sent within 24 hours;

(b) Monthly "No Hit" alerts, if applicable;

(c) Identity theft insurance; and

(d) Fraud resolution services in which a ProtectMyID agent walks you through resolving identity theft.

14. Does ProtectMyID Elite monitor all three credit bureaus?

No, ProtectMyIDElite monitors only the Experian credit file, not the credit files of Transunion or Equifax. However, Experian has the largest credit file of the three national credit bureaus.

15. How do I activate the credit monitoring service?

Please visit www.protectmyid.com/protect and enter the activation code provided to you. You will be instructed on how to initiate your online membership. If you have any difficulty accessing this product on-line, please call Experian at (866) 751-1324 for assistance.

16. Is there a deadline to enroll in ProtectMyID Elite?

Yes. Individuals should promptly decide whether they wish to enroll. The deadline for enrolling is September 30, 2016.

17. What should I do if I receive a credit monitoring report?

If there are no changes to your credit report during a particular month, you will receive an "all clear" report for that month. In that case, there is nothing that you need to do.

If you receive a report other than an "all clear" report, the report will reflect certain credit activity in your name that's commonly associated with identity theft, such as applying for a new credit card or loan, a change of address, *etc.* If the transaction isn't one you initiated, simply call ProtectMyID toll free and Experian will immediately put you in touch with a fraud resolution agent to find out what's happening and work to correct the problem.

18. I haven't noticed any suspicious activity, but what can I do to protect myself and prevent being victimized by identity theft?

In addition to enrolling in Experian's ProtectMyID service, consider taking the following measures:

- **Review your credit reports**. You can receive free credit reports by placing a fraud alert as described below. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three national credit bureaus. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report from one of the three credit bureaus every four months.

- **Review your account statements.** You should carefully review for suspicious activity the statements that you receive from credit card companies, banks, utilities and other service providers.

- **Respond to suspicious activity.** If you receive an e-mail or mail alert from Experian, contact an Experian fraud resolution representative at (866) 751-1324. If you notice suspicious activity on an account statement, report it to your credit card company or service provider and consider closing the account. You also should consider reporting such activity to your local police department, your state's attorney general, and the Federal Trade Commission. Importantly, **Experian will not contact you by telephone**. If you receive a telephone call from someone claiming to be from Experian, please contact an Experian representative immediately at (866) 751-1324.

- **Consider placing a fraud alert with one of the three national credit bureaus.** You can place an initial fraud alert by contacting one of the three national credit bureaus listed below. For 90 days, an initial fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(888) 766-0008	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

19. What should I do if I detect suspicious or unusual activity?

Your first point of reference should be to the written materials received in the Notice Letter. Alternately, you should call Experian at (866) 751-1324.

Questions About Identity Theft

20. What is identity theft?

According to the United States Department of Justice, the terms identity theft and identity fraud "refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain."

21. Am I at risk of identity theft?

We cannot eliminate the possibility that someone might access the information and attempt to misuse it. Consequently, the Company sent you a notice about the incident to make you aware of the situation and to permit you to take advantage of the ProtectMyID service that the Company has arranged. You should consider activating ProtectMyID to reduce the risk that you will be victimized by identify theft and to protect yourself if identity theft does occur.

22. Do I need to cancel my credit cards and change bank/checking accounts?

As far as we are able to determine, your credit card and financial account information are not at risk. However, you should still check your credit reports, credit card statements, and financial account statements for suspicious activity. If you do observe any suspicious activity, you should contact Experian at (866) 751-1324 for assistance.

23. Has anyone been victimized by identity theft because of this incident?

To date, we are not aware that anyone has been victimized by identity theft because of this security incident.

24. What do I do if I learn that my identity has been misused?

Contact Experian, explain the situation, and tell them you would like to use their ProtectMyID services.

File a police report with your local police or the police in the community where the identity theft took place. Get a copy of the report or at the very least, the number of the report to submit to creditors and others who

may require documentation of the crime.

File a complaint with the Federal Trade Commission. The FTC maintains a database of identity theft complaints which can be accessed by law enforcement agencies for investigations. You can report identity theft at www.ftc.gov/idtheft or by calling the following toll-free number: (877) ID-THEFT (438-4338).

For more information on recovering from identity theft and help with specific problems, read "Taking Charge: What to Do if Your Identity is Stolen," a publication from the FTC. It's available online at www.ftc.gov/idtheft (specific link is: https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf) or you can call (877) ID-THEFT to order a free copy.

If you observe suspicious activity, contact your creditors immediately. Ask to speak to someone in the security or fraud department, and follow-up in writing. If you discover a changed billing address on an existing card, close the account immediately. When you open a new account, ask that a password be required before any inquires or changes can be made on the account. When selecting a password or personal identification number avoid using easily available information or any of the information related to your name or Social Security number.

25. Where can I find more information about data security and identity theft?

The resources below provide information about data security, privacy protection and identity theft:

- Your state attorney general
- Federal Trade Commission ID Theft Information
- Identity Theft Resource Center
- The Privacy Rights Clearinghouse

Questions About Free Credit Reports

26. How do I request a copy of my credit report?

You can request a copy of your credit report yourself once a year from each of the three main credit bureaus through the Annual Credit Report Request Service by calling (877) 322-8228 or by visiting www.annualcreditreport.com. Many people choose to stagger their requests so that they receive a copy from one of the agencies every four months.

27. Do I have to pay for the credit report?

No. You can order your credit reports from all three credit bureaus for free once a year.

28. What should I look for in my credit report?

When reviewing your credit reports, be on the lookout for suspicious activity including:

- Inquiries from companies you haven't contacted or done business with;
- Purchases or charges on your accounts you didn't make;
- New accounts you didn't open or changes to existing accounts you didn't make; and
- Address where you never lived in the "Personal Information" section.

29. What are other signs that I might be a victim of ID theft?

- Bills that do not arrive as expected;
- Unexpected credit cards or account statements;
- Calls or letters about purchases you did not make; and
- Denials of credit for no apparent reason.

30. How often should I order new credit reports and how long should I go on ordering them?

It might be a good idea to order copies of your credit reports every three or four months for a while. How long you continue to order them is up to you. Identity thieves usually, but not always, act soon after stealing personal information. Thereafter, consider checking your credit reports at least twice a year as a general privacy protection measure.

Questions About Fraud Alerts

31. What is a fraud alert?

A fraud alert tells creditors to contact you before opening any new accounts or changing your existing accounts. Once you notify one of the three national credit bureaus of your fraud alert, the others will be notified to place a fraud alert as well. All three credit bureaus also will send you one credit report, free of charge.

32. Can I place a fraud alert on my credit report?

Yes. You can contact any of the three national credit bureaus at the following telephone numbers or URLs:

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

If you call just one of the bureaus, they will notify the other two. A fraud alert will be placed on your file with all three, and you will receive a confirming letter from all three.

33. Are there drawbacks to placing a fraud alert?

A potential drawback to activating a fraud alert would occur should you attempt to open a new account. You would need to be available at either your work phone number or home phone number in order to approve opening the new credit account. If you are not available at either of those numbers, the creditor may not open the account. In addition, it may take longer to obtain credit and in some cases merchants may be hesitant to open a new account.

Fraud alerts will not necessarily prevent someone else from opening an account in your name. A creditor is not required by law to contact you if you have a fraud alert in place. If you suspect that you are or have already been a victim of identity theft, fraud alerts are only a small part of protecting your credit. You also need to pay close attention to your credit report to make sure that the only credit inquiries or new credit accounts in your file are yours.

34. Does placing a fraud alert on my account damage my credit?

No, placing a fraud alert does not damage your credit.

35. Will a fraud alert stop me from using my credit cards or obtaining new credit?

No, it will not stop you from using your credit cards. However, it may slow the process of obtaining new credit. Since the purpose of the fraud alert is to protect you from allowing someone else to open credit in your name, creditors will need to re-verify the identity of the person applying for credit.

36. How long does a fraud alert last?

An initial fraud alert lasts 90 days. You can remove an alert by calling the credit bureaus at the phone number given on your credit report. If you want to reinstate the alert, you can do so.

37. Can I extend a fraud alert placed on my credit file?

You may extend a free 90-day fraud alert by reinstating the alert when it expires. There is no limit to the number of times a free alert can be placed on your account, but the responsibility for reinstating the alert rests with you.

38. I called the credit bureau fraud line and they asked for my Social Security number. Is it okay to give it?

The credit bureaus ask for your Social Security number and other information to identify you and avoid sending your credit report to the wrong person. It is okay to give this information to the credit bureau when you call them.

Questions About A Security Freeze

39. What is a security freeze and how do I place one on my credit file?

A security freeze means that your credit file cannot be shared with potential creditors or other persons considering opening new accounts unless you decide to unlock your file by contacting a credit reporting agency and providing a PIN or password. Most businesses will not open credit accounts without first checking a consumer's credit history. If your credit files are frozen, even someone who has your name and Social Security number would not likely be able to get credit in your name.

40. Do you recommend that I place a security freeze?

The security freeze (or credit freeze) is an option generally best reserved for people who have experienced extreme ID theft. Because the freeze essentially locks down your credit, it can be inconvenient for people who are simply seeking extra protection for their credit.

41. I currently have a security freeze/lock on all my credit reports. Can I still do credit monitoring?

Yes, most states with credit freeze legislation provide an exemption so that credit monitoring can occur. If you reside in one of these states, there may be an extra "verification" step for you to complete during monitoring activation, but the monitoring should still be activated. Because credit freeze laws are being written into law constantly nationwide, we are not able to let you know what your state's specific exemptions are. We recommend researching the issue on the credit bureaus' websites or on sites explaining your state's freeze legislation. If you have the time, it might be worth it just to try the monitoring and see if it goes through. To learn more, contact your State Attorney General's office or visit the Federal Trade Commission's website at www.ftc.gov/idtheft and click on the link for credit freeze information.

Other Questions

42. Should I contact the Social Security Administration and change my Social Security number?

The Social Security Administration very rarely changes a person's Social Security number. The mere possibility of fraudulent use of your Social Security number would probably not be viewed as a justification. There are drawbacks to changing your Social Security number. The absence of any history under the new Social Security number would make it difficult for you to get credit, continue college, rent an apartment, open a bank account, get health insurance, etc. In most cases, getting a new Social Security number would not be a good idea.

Firmwide:140870768.1 999999.1956