NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
Tabor Center
1200 17th Street, Suite 1000
Denver, Colorado 80202-5835
United States

Direct line +1 303 801 2732
david.navetta@nortonrosefulbright.com

Tel +1 303 801 2700
Fax +1 303 801 2777
nortonrosefulbright.com

March 14, 2017

By Certified Mail
Return Receipt Requested

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

I write on behalf of my client, InMoment, Inc., to inform you of a security incident involving personal information that affected one (1) New Hampshire resident. InMoment, Inc. is notifying the affected individuals and outlining some steps they may take to help protect themselves.

On February 27, 2017, an unauthorized individual, impersonating an InMoment, Inc. executive, contacted an InMoment, Inc. employee requesting 2016 W-2 information for certain current and former InMoment, Inc. employees. Unfortunately, before it was determined that the request was fraudulent, the employee provided these files that contained limited information about some of our current and former employees. This incident was discovered the same day—February 27, 2017.

InMoment, Inc. takes the privacy of personal information seriously, and deeply regrets that this incident occurred. Affected individuals have been notified, which includes an offer for two years of complimentary identity protection and fraud resolution services, and instructions on how to prevent or remedy any fraudulent tax returns filed in their names. A copy of the notice being sent to the affected New Hampshire resident today is included for your reference.

If you have any questions or need further information regarding this incident, please contact me at (303) 801-2732 or david.navetta@nortonrosefulbright.com.

Very truly yours,

David Navetta
Partner
Co-Chair, Data Protection, Privacy & Access to Information

DJN/smm
Enclosure

[INSERT NAME]

[DATE]

[ADDRESS]

Dear [NAME],

Notice of Data Breach

As explained in a prior email communication, InMoment, Inc. recently became aware of a security incident possibly affecting the personal information of certain current and former InMoment employees. We are providing this notice as a precaution to formally inform potentially affected individuals of the incident and to call their attention to some steps they can take to help protect themselves. We sincerely apologize for any frustration or concern this may cause you.

What Happened

Based upon our investigation, it appears that on January 27, 2017, an unauthorized individual, impersonating an InMoment executive, contacted an InMoment employee requesting 2016 W-2 information for certain current and former InMoment employees. Unfortunately, before it was determined that the request was fraudulent, the employee provided these files that contained limited information about some of our current and former employees.

What Information Was Involved

The W-2 files contained employee information including first and last name, addresses, Social Security number and 2016 compensation and deduction information. Employees' dates of birth were not provided. Based on our investigation, we have not found any evidence that this incident involves any unauthorized access to or use of any InMoment computer system or network and no further information about any employee or customer was provided to any unauthorized individual. Please note, at this time, we are not aware of any fraud or misuse of your information as a result of this incident.

What We Are Doing

InMoment takes the privacy and protection of personal information very seriously, and deeply regrets that this incident occurred. We took steps to address this incident promptly after it was discovered, including working to investigate and remediate the situation. We will also provide annual training to our employees on the proper use of sensitive information and how to recognize email scams; provide periodic updates to employees throughout the year as new phishing schemes or email scams come to our attention; and provide additional training concerning how to handle any requests for sensitive information and how to potentially recognize a phishing scheme for employees in departments or functions with access to sensitive employee information. In addition, we have contacted law enforcement and will continue to cooperate in their investigation of this incident.

In addition, to help protect your identity, we have offered you two years of complimentary identity protection services from a leading identity monitoring services company. These services help detect possible misuse of your personal information and provide you with superior identity protection support focused on immediate identification and resolution of identity theft. For more information about these services and instructions on completing the enrollment process, please refer to the email you already received regarding these services.

What You Can Do

We want to make you aware of steps you can take to guard against fraud or identity theft. You can carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. Also, the "Information about Identity Theft Protection" reference guide, included here, describes additional steps that you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

It is possible that the unauthorized individual who obtained the W-2 information could try to file a fraudulent tax return in your name. Accordingly, you may wish to call the IRS Identity Protection Specialized Unit hotline at 1-800-908-4490. As an additional precautionary measure, you may also wish to file a Form 14039 "Identity Theft Affidavit" with the IRS to help prevent someone from filing a fraudulent tax return in your name. For additional information from the IRS about identity theft, please visit https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft or call 800-908-4490. There may also be similar resources and forms to file for individual states, which can be obtained by contacting your state department of revenue directly for more information.

For More Information

For more information about this incident, or if you have additional questions or concerns about this incident, you may contact us directly at 801-743-7588 between 9:00-5:00 Mountain time, Monday through Friday or via email at dpowell@inmoment.com. Again, we sincerely regret any concern this event may cause you.

Sincerely,

David Powell

Information about Identity Theft Protection

To help protect your identity, we have arranged for two years of complementary Identity Restoration assistance and fraud detection services through Experian. For more information about these services and instructions on completing the enrollment process, please refer to the email you already received regarding these services.

Review Accounts and Credit Reports: You can also regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For additional information from the IRS about identity theft, please visit https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft or call 800-908-4490. There may be similar resources available at the state level, and you can contact your state department of revenue directly for more information.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)
General Contact:
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:
P.O. Box 740256, Atlanta, GA 30374

Credit Freezes:
P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
General Contact:
P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
General Contact:
P.O. Box 105281
Atlanta, GA 30348
800-888-4213

Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872

From: Mark Webb [mailto:mwebb@inmoment.com]
Sent: Wednesday, March 01, 2017 12:26 PM
To: Mark Webb
Subject: Data Breach - Please Read

We have learned that InMoment was the victim of a data-security incident which affects your personal information.

We take this matter and the security of personal information very seriously at InMoment, and the company is taking steps to help you protect against the possible misuse of your personal information.

We are paying for identity protection services from an identity monitoring services company. We are in the process of arranging these services and further information about how you sign-up for these services will be provided in a separate communication.

We also want to provide you with information about this incident so you can take steps to guard against fraud or identity theft. Currently, it appears that the information that would appear on your W-2 was compromised. This would include your name, address, social security number, and 2016 earnings and taxes.

It is possible that the unauthorized party who obtained the information could try to file a fraudulent tax return in your name. This is a common form of fraud being perpetrated this time of year.

1. We recommend that you call the IRS Identity Protection Specialized Unit hotline at 1-800-908-4490. If a fraudulent return has already been filed in your name, the IRS can act to cancel the fraudulent filing.

2. If no return has been filed in your name, you should consider filing your 2016 return as soon as possible.

3. In addition, we are providing an IRS Form 14039 "Identity Theft Affidavit" that can be filed with the IRS to also help prevent someone from filing a fraudulent tax return in your name.

4. The IRS hotline representative may also have additional recommendations for how to protect yourself.

For additional information from the IRS about identity theft, please visit https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.
There may also be similar resources and forms to file for individual states, so we recommend that you check directly with your state department of revenue for more information.

Credit Reports:

1. We recommend checking your credit reports for accounts you did not open or for inquiries from creditors you did not initiate.

2. If you see anything you do not understand, call the credit agency immediately.

3. You may also consider placing a Fraud Alert or Credit Freeze on your file to help prevent fraud.

For more information about these options, contact the credit bureaus using the contact information below.

✓ Equifax (www.equifax.com): 800-685-1111

✓ Experian (www.experian.com): 888-397-3742

✓ TransUnion (www.transunion.com): 800-888-4213

For additional information on steps you can take to help protect yourself, you can contact the FTC at Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft or visit https://www.identitytheft.gov.

We will update you as soon as we have a credit monitoring service in place. Obviously, time is of the essence and we will move as quickly as possible to ensure your protection. We will continue to review and enhance our security practices to further secure our systems.

If you have questions in the meantime, please feel free to contact me or David Powell.

Like you, we too are frustrated with these types of cybercrimes that are so prevalent in today's society, and to the extent we can, we will help alleviate the impact to you.

Mark Webb
CFO InMoment

From: David Powell [mailto:dpowell@inmoment.com]
Sent: Tuesday, March 14, 2017 9:27 AM
To: [redacted]
Subject: Data Security Incident Follow-Up Message

Hello [redacted]

I am writing to follow up on the email Mark sent Wednesday regarding our data-security incident. In an effort to proactively protect each employee, we have now arranged two services for you through Experian. The first is *Identity Restoration Assistance*, and the second is *Fraud Detection Services*. InMoment has paid 100% of the fees associated with these services.

Service #1 – *Identity Restoration Assistance*: (This service is available to you whether or not you enroll in Service #2 below).

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **877-890-9332**. Be prepared to provide engagement number **DB00776** as proof of eligibility for the *Identity Restoration Services* by Experian. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). ** Please note that this offer is available to you for two years from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration . You will also find self-help tips and information about identity protection at this site.

Service #2 – *Fraud Detection Services* (***IdentityWorks***^{SM}). While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks^{SM} as a

complimentary two-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by: March 12, 2019** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bplus2
- Provide your **activation code**: [redacted]

24-MONTH EXPERIAN IDENTITYWORKS Membership:

✓ A credit card is **not** required for enrollment in Experian IdentityWorks.
✓ **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.
✓ **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
✓ **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
✓ **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
✓ **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
✓ **$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, **please** contact Experian's customer care team at 877-890-9332 by **March 12, 2019.** Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

Please refer to www.ExperianIDWorks.com/restoration for more information.

Should you have questions or concerns regarding this matter, please do not hesitate to contact me or Mark Webb.

Sincerely,

David Powell

David S Powell
VP, Human Resources
310 East 4500 South, Murray, UT 84107
P:801-743-7588 C:801-918-0667
