RiskAware

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
LINCOLN LABORATORY
244 WOOD STREET
LEXINGTON, MASSACHUSETTS 02420-9108

March 16, 2023

Hello

RiskAware has received your follow up to our incident reporting and appreciate the importance and high standards in place for our maintaining data privacy. In 17 years, RiskAware has not written a breach letter. The error was a human error. The employee attached the wrong file to two email communications and did not first check it, which is against our practice. We have educated the employee, documented the process failure for his HR file with us, and have held a company team meeting to expose the process failure and reinforce our expectations on the importance of following procedures and the risks to the applicant, client, and our company when we don't. We reduced the employee's duties and added supervision to ensure we see better due diligence from the employee going forward.

In follow up to the self-reported incident, below describes our handling and next step efforts with the applicant, the applicant's employer with whom PII was shared, with MIT LL, and with the State of MA.

RISKAWARE'S APPLICANT EFFORTS TO COMMUNICATE AND REMEDIATE POSSIBLE DATA BREACH: At this point we have contacted and talked directly to the two applicants personally by phone and in writing. We have extended information about Identity Theft, have offered remediation and credit monitoring. Neither of the two applicants involved in our Incident report have indicated any concern that data was breached, or a further need for remediation as of now, since both indicate their current employer's HR contact to whom the PII information was inadvertently sent, did already know and have full access to the data contained on the application in the employee's HR company records.

RISKAWARE'S EMPLOYER EFFORTS TO COMMUNICATE AND REMEDY POSSIBLE DATA BREACH: RiskAware has also confirmed directly with both Employer HR contacts to whom PII was erroneously sent, that the application data did not leave their possession and was destroyed without furtherance. In addition, both HR Contacts independently confirmed that the PII data indicated by the application (Full Name, Address History, Phone Number, Email, SSN, DOB, and Driver License Number) is data already known to the company and diminished the ide with us that this was a breach. Nonetheless, per our request the information was immediately shredded and/or deleted from electronic records (email) to ensure its destruction. Both contacts assured us in our follow up with them that the information was not viewed or forwarded elsewhere. This confirmation is reassuring that information went no further and was not put in subsequent risk.

RISKAWARE'S MIT LINCOLN LABORATORY DATA BREACH COMMUNICATIONS AND EFFORTS: In full compliance with our responsibilities to MIT LL as our client and per our meaningful and important contract, RiskAware did within a few hours of our discovery of our company error, disclose the breach of information. Our communications (see below) described what happened and our steps taken to reach the individuals to whom PII was erroneously sent (see above) to contain the incident to the individual involved, and to ensure immediate information destruction. RiskAware also contacted the Incident Security Hotline, and our Security Team points of contact at MIT LL, Frank Legere and Zachary Grande. We have replied to email follow up requests to assure our contact directly with the applicants and confirmations that information was

destroyed. We have indicated our cooperation with any investigation and follow up with the State of Massachusetts. RiskAware did make a mistake, but we did not try to cover it or ignore it. We hope that in review of this incident against our performance under this contract now and in the past, these factors may continue to be considered, as indication of our company character and responsibility to our contract obligations and duties.

RISKAWARE'S EFFORTS TO COMMUNICATE OUR DATA BREACH WITH THE STATE OF MASSACHUSETTS:
Finally RiskAware did reach out to the State of MA to confer that we were reported by MIT Lincoln Laboratory for breach. We were directed on follow up and have sent the attached letters to Massachusetts' Office of Consumer Affairs and Business Regulation, as a requirement of our follow up. We will comply with any next step as directed by the State of Massachusetts.

This has been a very difficult chapter for our company, as minimal as this breach turned out to be in scale. We were fortunate that the employer did have possession of the application information shared, but realize the need for added care on our end. Since we have agreed to handle paper CBI applications from MIT Lincoln Laboratory, we know we must be very deliberate in our handling and supervising the the task of breakup of these forms into Release only documents, to better remove the potential for attachment of the full file in the future. Our own 360 Review process has assured our full company focus on what happened and how we can prevent any further occurrence by applying our existing practices, adding further process rigidity, and team member supervision. But what we most want to support is that this incident is not our company DNA. We respect all applicant's information and understand our duty to keep it safe. This is very personal to us and very humbling. Please let me know if there is anything further we can do to demonstrate compliance with our contract and responsibilities.

Sincere Regards;

Christine Prespare
Director of Business Development
RiskAware
cprespare@riskaware.com
(o) 877-552-8907 x 5
(c) 614-260-9729
www.riskaware.com

RiskAware

March 9, 2023

O[redacted] A[redacted]
[redacted], [redacted]

Dear O[redacted],

On behalf of RiskAware's organization we are writing to inform you that when verifying your employment our company made a processing error which may or may not have breached your information.

Why am I receiving this?
A data security incident has surfaced. You may or may not have been affected, but we want to make you aware of the incident and inform on ways you can further protect yourself if needed.

What happened?
Your submitted application for unescorted access to [redacted] was shared while attempting to verify your employment. This exposed the following fields of information about you: ***Name (including middle name), Address History, Phone Number, Email, Date of Birth, Social Security Number, and Driver's License***.

What should you do?
RiskAware will support any required effort to mitigate the impact of our mistake. You have the right to contact law enforcement to file a report. Also, you can request a security freeze free of charge by utilizing the following links:

- https://www.transunion.com/credit-freeze
- https://www.equifax.com/personal/credit-report-services/credit-freeze/
- https://www.equifax.com/personal/credit-report-services/credit-freeze/

In addition, at RiskAware's expense, we can provide you with Credit Monitoring. We have enclosed the document "Remedying the Effects of Identity Theft" that further describes your rights and protections.

We have informed [redacted] and your employer [redacted], through the HR contact to whom the application was sent to report this incident and will work cooperatively as needed with any organization including Massachusetts Office of Consumer Affairs and Business Regulation.

If you would like more information about this incident or to move forward with Credit Monitoring, please contact us or reach me personally at (877) 552-8907 x 112. Once more, we sincerely apologize for our mistake, and please know of our meaningful desire to provide any needed remediation.

Regards,

Christine Prespare
Director
RiskAware LLC

RiskAware

March 9, 2022

E B
[redacted]

Dear [redacted]n,

On behalf of RiskAware's organization we are writing to inform you that when verifying your employment our company made a processing error which may or may not have breached your information.

Why am I receiving this?
A data security incident has surfaced. You may or may not have been affected, but we want to make you aware of the incident and inform on ways you can further protect yourself if needed.

What happened?
Your submitted application for unescorted access to [redacted] was shared while attempting to verify your employment. This exposed the following fields of information about you: ***Name (including middle name), Address History, Phone Number, Email, Date of Birth, Social Security Number, and Driver's License***.

What should you do?
RiskAware will support any required effort to mitigate the impact of our mistake. You have the right to contact law enforcement to file a report. Also, you can request a security freeze free of charge by utilizing the following links:

- https://www.transunion.com/credit-freeze
- https://www.equifax.com/personal/credit-report-services/credit-freeze/
- https://www.equifax.com/personal/credit-report-services/credit-freeze/

In addition, at RiskAware's expense, we can provide you with Credit Monitoring. We have enclosed the document "Remedying the Effects of Identity Theft" that further describes your rights and protections.

We have informed [redacted] and your employer, [redacted], through the HR contact to whom the application was sent to report this incident and will work cooperatively as needed with any organization including Massachusetts Office of Consumer Affairs and Business Regulation.

If you would like more information about this incident or to move forward with Credit Monitoring, please contact us or reach me personally at (877) 552-8907 x 112. Once more, we sincerely apologize for our mistake, and please know of our meaningful desire to provide any needed remediation.

Regards,

Christine Prespare
Director
RiskAware LLC