LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Allen E. Sattler
650 Town Center Drive, Suite 1400
Costa Mesa, California 92626
Allen.Sattler@lewisbrisbois.com
Direct: 714.668.5572

April 12, 2021

File No. 28310.1045

VIA WEBSITE PORTAL

Maine Department of Professional and
Financial Regulation
Bureau of Insurance
34 State House Station
Augusta, ME 04333

Re: Notification of Data Security Incident

Dear Maine Department of Professional and Financial Regulation:

We represent Iscential Inc. ("Iscential") in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify your office of the incident in accordance with 10 M.R.S. §§ 1346 – 1350.

1. **Nature of the Security Incident**

Iscential is an independent insurance agency, risk management, and financial services agency headquartered in Houston, Texas. On November 16, 2020, Iscential discovered that the email account of a single employee was potentially compromised as a result of an email phishing attack. Iscential immediately blocked and reset that email user account. On November 18, 2020, Iscential engaged an independent computer forensic firm to determine what happened. In December 2020, the computer forensic firm concluded that Iscential's email tenant was indeed compromised, but the scope of that compromise was limited to the one email user account referenced above. Moreover, the period of compromise for that account was limited in duration to less than one day.

Accordingly, acting in the abundance of caution, on January 22, 2021, Iscential engaged with a third-party vendor to perform a data mining review of the single compromised mailbox in order to determine what and whose personal information may have been accessed by the unauthorized user.

On March 12, 2021, Iscential and its vendor concluded their comprehensive review and developed a list of individuals whose personal information may have been accessed as a result of this incident.

On April 12, 2021, Iscential provided individual notification to all potentially affected individuals by mailing notification letters to their last known address.

2. Type of Information and Number of Maine Residents Involved

The incident involved the personal information for approximately 2 Maine residents. The information involved in the incident may differ depending on the individual but may include name, address, date of birth, Social Security number, driver's license or state identification number, financial account information, and credit/debit card information. For a small subset of affected individuals, the information may have also included health information. A sample copy of the notification letter to be sent to the affected individuals is submitted with this correspondence.

3. Measures Taken to Address the Incident

In response to the incident, Iscential retained cybersecurity experts and launched a forensic investigation to determine the source and scope of the compromise. Iscential is in the process of implementing additional security measure to further harden its digital environment in an effort to prevent a similar event from occurring in the future.

In addition, Iscential has reported the incident to the Federal Bureau of Investigation ("FBI") and will cooperate fully to assist with any investigation.

Furthermore, Iscential is notifying the affected individuals and providing them with steps they can take to protect their personal information, including by enrolling in the complimentary credit monitoring and identity protection services that are offered in the notification letter.

4. Contact Information

Iscential is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact Allen Sattler at 714-668-5572 or Allen.Sattler@lewisbrisbois.com.

Sincerely,

Allen E. Sattler of
LEWIS BRISBOIS BISGAARD & SMITH LLP

AES

Encl.: Notification Letter Template

cc: Loree Stuck, Lewis Brisbois (Loree.Stuck@lewisbrisbois.com)
Vy Nguyen, Lewis Brisbois (Vy.Nguyen@lewisbrisbois.com)

Iscential Inc.

C/O IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-833-903-3648
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

April 12, 2021

Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

We are writing on behalf of Iscential Inc. ("Iscential") to provide you with information about a recent data security incident that may have impacted your personal information. The privacy and security of your personal information is extremely important to us. We are sending you this letter to notify you of this incident and to inform you about steps you can take to help protect your personal information.

What Happened? On November 16, 2020, Iscential discovered that the email account of a single employee was potentially compromised as a result of an email phishing attack. Iscential immediately blocked and reset that email user account.

On November 18, 2020, Iscential engaged an independent computer forensic firm to determine what happened. In December 2020, the computer forensic firm concluded that Iscential's email tenant was indeed compromised, but the scope of that compromise was limited to the one email user account referenced above. Moreover, the period of compromise for that account was limited in duration to less than one day.

Accordingly, acting in the abundance of caution, on January 22, 2021, Iscential engaged with a third-party vendor to perform a data mining review of the single compromised mailbox in order to determine what and whose personal information may have been accessed by the unauthorized user. On March 12, 2021, Iscential and its vendor concluded their comprehensive review and developed a list of individuals whose personal information may have been accessed as a result of this incident.

While we are unaware of the misuse of any information involved with this incident, we are writing to inform you about the incident and to provide you with complimentary credit monitoring services.

What Information Was Involved? Based on our investigation, the following information may have been accessed as a result of the incident: <<variable text>>

What We Are Doing. As soon as we discovered the incident, we took the steps discussed above. We also consulted with IT experts and took the recommended steps to enhance the security of our environment in order to help prevent a similar incident from occurring in the future. Finally, out of an abundance of caution, we are offering you twelve (12) months of identity theft protection services provided by IDX, a company specializing in fraud assistance and remediation services.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do. We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-903-3648 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is July 12, 2021.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information. You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-903-3648 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have.

Sincerely,

Mark Michels
Director of Claims Management
Iscential Inc.

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-903-3648 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A 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:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.