KDG | KAUFMAN DROZDOWSKI & GRENDELL, LLC
ATTORNEYS AT LAW

VIA FEDERAL EXPRESS
Office of the Attorney General of New Hampshire (The Honorable John M. Formella)
33 Capitol Street
Concord, New Hampshire 03301
Doj.cpb@doj.nh.gov

Subject: Data Base/Security Breach Notification

To Whom it May Concern:

This letter is sent to notify the Attorney General's office and its Department of Justice of a Data Base/Security Breach that occurred at Vincent Lighting Systems Company ("Vincent") and is intended to satisfy the requirements of N.H. Rev. Stat. §§ 359-C: 19 et seq. Undersigned represents Vincent and provides a summary of relevant facts below.

Vincent is located in Solon, Ohio and employs approximately fifty (50) people. The Company provides, among other things, theatrical and event lighting products, support and services.

Vincent recently experienced a data breach involving unauthorized access to its computer systems, which appears to have occurred on February 13, 2023 when Vincent received a "ransom" message from an unauthorized user ("Unauthorized User"). Upon learning of this situation, Company representatives immediately notified the local office of the Federal Bureau of Investigation (FBI) and have learned through those communications that the person or organization that committed this crime is already under investigation by the FBI. The Company's understanding is that this incident was part of a "day zero" event in which the Unauthorized User employed techniques and technology used for the first time just days before the unauthorized access affecting Vincent's systems. In addition to notifying the FBI, the Company also immediately began an investigation to determine the scope and details of the unauthorized access.

Based upon the investigation to date, it now appears that Personal Information (as defined in New Hampshire) of a single New Hampshire resident may have been among information accessed by the Unauthorized User. The fact that this individual who resides in New Hampshire was possibly impacted by this event was not immediately apparent, and the Company has not seen evidence

confirming that the Personal Information of the New Hampshire resident or anyone else has actually been misused or was specifically targeted. Regardless, Vincent proceeded to notify this person, along with others outside of New Hampshire whose Personal Information may have been impacted by this event. The Notice template mailed on April 4, 2023 is attached for your convenient reference, and includes additional information and details regarding this matter, including additional steps Vincent is taking to address it. As you will see, the Notice letter includes an offer to provide the affected New Hampshire resident (and others outside New Hampshire) with two-years (24 months) of identity theft protection from an outside vendor at no charge or cost, among other protection and guidance that the letter describes.

As noted above, this letter is intended to satisfy New Hampshire's statutory requirements for Notice of this event. If, however, the Attorney General's office should have questions or require any additional information regarding this matter, please do not hesitate to contact me at .

Thank you for your attention to this matter.

Sincerely,

Shawn M. McGraw (Ohio Bar No. 0063547)
Member
Kaufman, Drozdowski & Grendell LLC

10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

>>Name 1>><<Name2>>
>>Address1>>
>>Address2>>
>>City>><<State>><<Zip>>
>>Country>>

April 4, 2023

Dear <<Name1>>:

Vincent Lighting Systems ("Vincent") is committed to protecting the privacy and security of the information we maintain. In that context, we are writing to inform you about a data security incident that may have involved some information related to you. This notice explains the incident that occurred, and the steps Vincent has and continues to take to address it.

What happened?

On February 13, 2023, Vincent discovered information indicating that a person or organization outside our company ("Unauthorized User") accessed our computer systems. Upon learning of this situation, we immediately disconnected our internal network from outside access and began an investigation.

As part of these events, we received contact information from the Unauthorized User along with a demand for payment for a key to remove encryption and to avoid publication of these matters. Vincent contacted the Federal Bureau of Investigation and informed the FBI of what occurred.

From our investigation, we have been able to determine that this attack encrypted servers and several back-ups, as well as some user workstations, but the Unauthorized User was unable to access several portions of our systems. As a result, the impact to ongoing business operations has been minimal and we did not negotiate with those who claim to have accessed our systems.

What information was involved?

Given the nature of these events, the exact nature of information that was accessed or acquired by the Unauthorized User is difficult to identify with precision at this time. Given that portions of our systems were accessed by the Unauthorized User, it is possible that your information (including Personal Information as defined by relevant laws) may also have been accessed, though we have not discovered any actual evidence or instances in which Personal Information has been misused to date. Personal Information, by way of illustration, might include information such as

.

What are we doing?

Vincent has and will continue to take several steps in response to this event. Beyond the immediate actions outlined above to assess what occurred and limit the impact, we felt it was important to notify you of what occurred consistent with applicable laws. We also felt it was appropriate to take additional steps. In this regard, we were already in the process of installing additional security measures within our systems when this event occurred and are continuing that work.

In addition, we are offering at no cost to you, identity theft protection services through IDX, a ZeroFox Company, which is an organization with well-recognized data breach and recovery services expertise. IDX identity protection services include: 24-months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully-managed identity 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 that we have arranged by calling or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided below. IDX representatives are available Monday through Friday from 6am – 6pm Pacific Time. Please note the deadline to enroll is .

We encourage you to take full advantage of this service offering. IDX representatives are aware of this situation and can answer any questions or concerns you may have regarding protection of your Personal Information.

To enroll:

Please call or visit
Enrollment Code: >>XXXXXXXXXX>>
You have until to activate your services.

After the 24-month period of complimentary service expires, if you take no additional steps, the Identity Theft Service IDX provides, as described above, will automatically expire with no additional action required by you. You will not be contacted or solicited by IDX and you will not be charged.

For More Information

You will find additional information and instructions for enrollment from IDX on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code above when calling or enrolling online with IDX, **so please do not discard this letter**.

Please call or go to for assistance or for any questions you may have. Additionally, if you have questions you wish to direct to Vincent, you can reach .

This incident is unfortunate, and we regret any concern or impact it may cause you. Please know we take this matter seriously. As noted above, we have and are continuing to evaluate this situation and implement additional measures where appropriate to enhance security of our data and business environment. We will also be doing additional training with our employees concerning data security so they can assist in identifying and helping prevent any similar incident from occurring in the future.

Sincerely,

Vincent Lighting Systems Company

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 1-800-939-4170 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 IDX 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 theft. 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.

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.

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.

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.