BROWNWINICK LAW

666 Grand Avenue | Suite 2000 | Ruan Center | Des Moines, Iowa 50309
515-242-2400 | 888-282-3515 | brownwinick.com

December 30, 2021

direct phone: (515) 242-2431
direct fax: (515) 323-8531
email: brian.mccormac@brownwinick.com

VIA U.S. FIRST CLASS MAIL & EMAIL
Office of the Attorney General
Consumer Protection and Antitrust
Gateway Professional Center
600 E. Boulevard Ave. Dept. 125
Bismarck, ND 58505
Email: ndag@nd.gov

Re: Notice of Data Security Incident

Dear Sir or Madam:

Our office represents Origin Design ("Origin") located at 137 Main Street, Suite 100, Iowa 52001. Pursuant to N.D.C.C. § 51-30-02, we are writing to notify your office of an event that may affect some personal information, as defined in N.D.C.C. § 51-30-01 (4), relating to one (1) North Dakota resident. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned after its submission.

Nature of the Data Event

On November 11, 2021, a group of cybercriminals known as Conti covertly infiltrated Origin's servers by exploiting an internet-connected mail server. On November 14, 2021, Conti shutdown Origin's servers and demanded an unspecified ransom to bring the servers back online. In other words, Conti initiated a ransomware attack. An investigation immediately began to secure our network, restore the servers, and determine if any confidential information could have been compromised or stolen. Our team was ultimately successful in securing and restoring the servers without communicating with Conti or paying any ransom. Our review found no evidence that Conti accessed company data or any documents containing personal information. After restoring its network, compiling all potentially accessed information, and obtaining contact information for all 285 of the potentially affected persons, Origin sent a full data breach notice on December 30, 2021.

Notice to North Dakota Resident

The documents in this data security incident related to the North Dakota resident we are notifying your office about included the following information: name, address, social security number, bank account number, routing number, and driver's license.

On December 30, 2021, Origin mailed written notices of this incident to all potentially affected

individuals, which includes the one (1) North Dakota resident. We have enclosed an anonymized version of the letter here as ***Exhibit A***.

Other Steps Taken and To Be Taken

In addition to alerting potentially affected persons about the incident, Origin has provided its employees and clients with guidance to help them stay vigilant about protecting their information and incidents of fraud. Origin recommended potentially affected persons review their account statements, monitor free credit reports, and report any suspicious activity or suspected incidents of identity theft to proper law enforcement authorities, including the Iowa Attorney General's office and the Federal Trade Commission (FTC). Origin provided the contact information for the three national credit reporting agencies and informed its employees and clients of their right to place a fraud alert and security freeze on their credit reports.

Origin is also offering all potentially affected persons identity theft protection services through ID Experts®. The services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. Origin has encouraged affected individuals to enroll and take full advantage of these services.

In response to this incident, we fully shut down our domain, decommissioned the breached server, rebuilt other servers involved in the breach, and removed all non-critical administrative rights and accounts. We also engaged a cybersecurity firm to offer recommendations on strengthening our network. These recommendations include adding further monitoring for network breaches, requiring multifactor authentication logins, establishing a plan to review all devices and accounts on a regular basis, training our staff to recognize threats, and continuing to follow industry best practices.

Contact Information

Origin takes the privacy and security of its information seriously and is committed to protecting its information. Should your office have any questions regarding this notification or other aspects of the data security event, please contact us at (515) 242-2400.

Sincerely,

Brian McCormac

Enclosure: Data Breach Notice Letter

December 30, 2021

«First_Name» «Last_Name»
«Address»
«CITY» «STATE» «ZIP»

NOTICE OF DATA BREACH

Dear «First_Name»,

We greatly appreciate your contributions to Origin Design in the past, and as a valued member of our team, we respect and protect the privacy of your information. We are writing to let you know about a data security incident that may involve unauthorized access to your identification information.

WHAT HAPPENED?

On November 11, 2021, a group of cybercriminals known as Conti covertly infiltrated Origin's servers by exploiting an internet-connected mail server. On November 14, 2021, Conti shutdown Origin's servers and demanded an unspecified ransom to bring the servers back online. This type of attack is called ransomware. An investigation immediately began to secure our network, restore the servers, and determine if any confidential information could have been compromised or stolen. Our team was ultimately successful in securing and restoring the servers without communicating with Conti or paying any ransom. Our review found no evidence that Conti accessed company data or any documents containing personal information. However, out of an abundance of caution, we want to alert you that certain information available on Origin's network was exposed to these unauthorized actors.

WHAT INFORMATION WAS INVOLVED?

Origin's network contained documents with your name, address, bank account number, routing number, social security number, and driver's license. Again, there is no evidence these documents were accessed, but they were present on the network during the breach.

WHAT WE ARE DOING

Origin values your privacy and deeply regrets that this incident occurred. We have a detailed plan to implement additional security measures and training designed to prevent a recurrence and to better protect the privacy of our valued employees and customers.

In response to this incident, we fully shut down our domain, decommissioned the breached server, rebuilt other servers involved in the breach, and removed all non-critical administrative rights and accounts. We also engaged a data security firm to offer recommendations on strengthening our network. These recommendations include adding further monitoring for network breaches, requiring multifactor authentication logins, establishing a plan to review all

devices and accounts on a regular basis, training our staff to recognize threats, and continuing to follow industry best practices.

FOR MORE INFORMATION

For further information and assistance, please contact President and CEO Pat Ready (563-599-9464, pat.ready@origindesign.com).

CONTACT YOUR FINANCIAL INSTITUTION

Because your bank account and routing numbers may have been accessed, we recommend that you contact your financial institution to notify them of the situation and change your account and routing numbers. As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained.

NOTIFY LAW ENFORCEMENT OF SUSPICIOUS ACTIVITY

As a precautionary measure, we recommend that you remain vigilant by reviewing your personal accounts. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including local authorities, the Iowa Attorney General's Office (1-888-777-4590), and the Federal Trade Commission (FTC), 600 Pennsylvania Avenue NW, Washington, D.C. 20580.

To report fraudulent activity with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Reports filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

WHAT YOU CAN DO

Finally, we are offering identity theft protection services through ID Experts® to provide you with MyIDCare™. MyIDCare 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, MyIDCare will help you resolve issues if your identity is compromised.

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and using the following Enrollment Code: . MyIDCare experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is March 21, 2022. We encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

We also recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting

http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

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

Experian
(888) 397-3742
www.experian.com
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
TransUnion LLC
P.O. Box 1000
Chester, PA 19016

FRAUD ALERTS & SECURITY FREEZES

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http:// www.annualcreditreport.com.

You may also want to consider using a security freeze. An initial security freeze is free. A security freeze prevents bad actors from opening financial accounts in your name by preventing creditors from accessing the information in your credit file needed to open an account. To use a security freeze, contact any of the three credit reporting agencies identified above.

We apologize for this incident.

Sincerely,

Origin Design
137 Main Street
Dubuque, IA 52001