



Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

RECEIVED

MAY 17 2019

CONSUMER PROTECTION

May 10, 2019

By Certified Mail

Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of Data Breach

Attorney General Gordon MacDonald:

I am writing on behalf of our client Condé Nast, to inform you of a data security incident that has affected approximately 6 New Hampshire residents. It appears that between April 14, 2019, and April 17, 2019, an unauthorized person or persons gained access to certain systems of the third-party vendor that maintains and operates certain subscription pages for Condé Nast ("Vendor"). The unauthorized person(s) appear to have used this access to modify certain subscription pages to acquire transaction information. This may have resulted in the compromise of names, postal addresses, email addresses, and payment card information (including card number, expiration date, and CVV) for individuals transacting on the affected subscription pages during the relevant period.

Condé Nast first learned of a potential incident on April 17, 2019, when a third-party provider of advertising services informed Condé Nast that there was a policy violation/malvertising on a subscription page. Condé Nast immediately began working with Vendor to assess the nature of the potential incident. The vulnerabilities were removed on April 17, 2019. On April 24, 2019, Vendor notified Condé Nast that it had a reasonable belief that the unauthorized code compromised transaction information. Condé Nast does not believe that the unauthorized person(s) continue to have access to Vendor's network or systems. Condé Nast is not aware of any evidence indicating that the unauthorized person(s) had access to systems other than those operated by Vendor.

While the investigation continues, Condé Nast's current understanding is that the incident potentially affected approximately 1,161 people, with 6 of those appearing to be New Hampshire residents. Vendor reports that it has reset all passwords used to access the systems impacted by the incident and that stronger password policies have been implemented. Condé Nast has arranged for Experian to provide one year of credit monitoring and identity protection services at no cost to US individuals who may have been affected by the incident. Information about how affected individuals can acquire these services and a description of the services is included in the consumer notice, which is enclosed.

Condé Nast notified affected individuals on May 10, 2019, and has notified law enforcement and financial institutions.

May 10, 2019

Please feel free to contact me if you have any questions or require additional information.

Sincerely,

A handwritten signature in blue ink, appearing to read "J Denvil".

James Denvil
Senior Associate
w.james.denvil@hoganiovells.com
+1 202 637 5521

Enclosures: Individual Notice

WIRED

Dear Subscriber,

We are writing to inform you of a cybersecurity incident that may have impacted a recent subscription transaction of yours with WIRED, a Condé Nast publication.

The WIRED subscription page is hosted by a third-party vendor. We believe that an unauthorized party accessed our vendor's systems in an attempt to acquire information about approximately 1,100 WIRED subscription transactions processed between April 14 and April 17, 2019. An investigation was undertaken and, by April 24, we learned that the information that may have been acquired included names, postal and email addresses, and credit/debit card numbers, security codes, and card expiration dates.

After first learning of the potential incident, we worked with our vendor to secure the subscription page and we notified law enforcement and credit/debit card companies about the incident. The vendor has since enhanced its security measures and is evaluating additional steps to prevent this type of incident from happening again.

Condé Nast values your business and we take the protection of your privacy seriously. We deeply regret that this incident occurred. In addition to the steps taken above with our vendor, we are also offering you one year of Experian's IdentityWorks credit monitoring and identity protection services at no cost to you.

What you can do to further protect yourself:

- As a precautionary measure, we recommend that you review your credit/debit card statements for any fraudulent charges and that you also review your credit report from one or more national credit reporting agencies indicated below.
- Although we have no indication at this time of unauthorized card use, we encourage you to enroll in the complimentary credit monitoring and identity protection services that we are offering. See

below for enrollment instructions.

- If you note any suspicious activity with your accounts, call your bank or payment card issuer.

Please read below for more information about the incident and how you can protect yourself. You can obtain more information about the breach by emailing condespecialservices@cdsfulfillment.com, calling toll-free at 800-234-3071, or writing to:

Conde Nast Special Services
PO Box 37617
Boone, IA 50037-0617
USA

Yours sincerely,
Condé Nast Cybersecurity

Notice of Data Breach

What Happened?

We believe that an unauthorized person or persons gained access to the systems of a third-party vendor that operates the subscription page for WIRED, a Condé Nast publication. The unauthorized person(s) used the access to modify the page's code in an attempt to acquire subscription transaction information, including names and credit/debit card numbers.

Upon discovering signs of a potential incident, our third-party vendor promptly initiated a forensic investigation, which is ongoing. Based on information received from the vendor on April 24, 2019, we believe that our subscription page was vulnerable between April 14, 2019, and April 17, 2019. The vendor has since enhanced its security measures and is evaluating additional steps to prevent this type of incident from happening again.

What Information Was Involved?

While the investigation continues, our current understanding is that the

incident involved the unauthorized access to credit/debit card information, including card numbers, security codes, expiration dates, names, postal addresses, and email addresses.

What We Are Doing.

We are notifying individuals who may have been impacted by the incident and offering them one year of Experian's IdentityWorks credit monitoring and identity protection services at no cost to them. We also have notified law enforcement and credit card companies about the incident. Our vendor engaged a forensic investigator to assess the scope of the incident and has enhanced its security measures.

What You Can Do.

We encourage you to enroll in the complimentary Experian IdentityWorks credit monitoring and identity protection services available. To activate your membership, please follow the steps below:

- Ensure that you **enroll by: August 30, 2019** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll:
www.experianidworks.com/credit
- If you note any suspicious activity with your accounts, call your bank or payment card issuer.
- Provide your activation code: **[Insert Code]**

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332. Be prepared to provide Engagement Number **DB12412** as proof of eligibility for the identity restoration services.

A credit card is **not** required to enroll in Experian's IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit-related fraud.
- **Up to \$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Please note that the Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part.

Even if you choose not to use the above services, we recommend that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and by checking your credit report from one or more of the national credit reporting agencies periodically. You are entitled to obtain a free annual credit report from each of the nationwide credit reporting companies—Equifax, Experian, and TransUnion. To do so, please go to www.annualcreditreport.com or call 1-877-322-8228. If you notice any suspicious activity, you should promptly report such activity to the proper law enforcement agencies.

We also recommend that you consider placing a fraud alert on your credit files. Adding a fraud alert to your credit report file makes it more difficult for someone to get credit in your name by requiring creditors to follow certain procedures. However, this may also delay your ability to obtain credit. No one is allowed to place a fraud alert on your credit report except you. To place a fraud alert on your file, contact one of the three nationwide credit reporting agencies; the first agency that processes your fraud alert will notify the others to do so as well.

You may also add a security freeze to your credit report file to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization. Agencies are required to place or remove freezes free of charge to the consumer. You can obtain information on fraud alerts and security freezes from the consumer reporting agencies and the Federal Trade Commission.

Equifax

P.O. Box 740241
Atlanta, GA 30374
www.equifax.com
1-800-525-6285

Experian

P.O. Box 9554
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion

Fraud Victim Assistance

P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report and 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 have rights under the federal Fair Credit Reporting Act. These include, among others, the right to know what is in your credit file; the right to dispute incomplete or inaccurate information; and the right to ask for a credit score.

You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center

600 Pennsylvania Avenue, NW

Washington, DC 20580

1-877-IDTHEFT (438-4338) / www.ftc.gov/idtheft

Iowa residents can contact the Iowa Office of the Attorney General at: Consumer Protection Division, Office of the Attorney General of Iowa, 1305 E. Walnut Street, Des Moines, IA 50319; (515) 281-5926; www.iowaattorneygeneral.gov (<http://www.iowaattorneygeneral.gov>).

Maryland residents can contact the Maryland Office of the Attorney General at: Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; <http://oag.state.md.us> (<http://oag.state.md.us>)

North Carolina residents can contact the North Carolina Attorney General at: North Carolina Office of the Attorney General 9001 Mail Service Center, Raleigh, NC 27699; (919) 716-6400; <https://www.ncdoj.gov> (<https://www.ncdoj.gov>)

Oregon residents can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301; (877) 877-9392; <https://justice.oregon.gov>.

Rhode Island residents can contact the Rhode Island Office of the Attorney General at: Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903; (401) 274-4400; <http://www.riag.ri.gov> (<http://www.riag.ri.gov>). Rhode Island residents have the right to obtain a police report and to request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (e.g., Social Security number, date of birth, and address) and proper identification (e.g., copy of a government-issued ID card and a bill or statement) prior to honoring your request.

All other residents can find information on how to contact your state attorney general at www.naag.org/naag/attorneys-general/whos-my-ag.php (<http://www.naag.org/naag/attorneys-general/whos-my-ag.php>).

For More Information.

If you have questions or concerns that are not addressed in this letter, please email condespecialservices@cdsfulfillment.com, call toll-free at

800-234-3071, or write to:

Conde Nast Special Services

PO Box 37617

Boone, IA 50037-0617

USA

[View this e-mail in your browser.](#)

View our [Privacy Policy](#)

[Unsubscribe](#)

Sent from Condé Nast, 1 World Trade Center, New York, NY 10007, attn: E-mail Coördinator

Copyright © 2019 Condé Nast. All rights reserved.