WILMERHALE

June 25, 2019

Jason C. Chipman
+1 202 663 6195 (t)
+1 202 663 6363 (f)
jason.chipman@wilmerhale.com

VIA FEDERAL EXPRESS
Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol St
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing to notify you of an incident of potential unauthorized access to the payment card information from certain recent event registrations using Cvent, Inc. ("Cvent") guest registration webpages. Cvent is a provider of software solutions to event planners, including online event registration.

Cvent is providing this notification on its own behalf and on behalf of its customers listed in Attachment A to the extent Cvent and/or these entities are required to notify your office under N.H. Rev. Stat. Ann. 359-C:20(I)(b). While the unauthorized activity only affected a limited subset of Cvent registrants, approximately 19 New Hampshire residents who registered for the identified entities' events may have been affected.

Cvent launched an investigation into suspicious code identified on an event registration page. Our investigation determined that a malicious unauthorized party was able to insert unauthorized code into a third-party extension utilized by our creative team on certain event registration webpages. The unauthorized code may have had access to certain consumer information submitted into some event guest registration websites between April 16 and May 30, 2019.

While Cvent will not be able to determine with certainty whether any individual's information was accessed by the unauthorized party, it is a possibility. Cvent assesses that the information involved in this incident may have included, at most, registrants' credit/payment card information (e.g., name, card number, expiration date, in some cases security code, and billing information). No other information was affected. Note that the investigation determined that, due to the functionality of the code, registrants who used Internet Explorer to register for an event would not have had their information accessed.

Cvent has identified the vulnerability, and the situation has been resolved. Cvent is working diligently to investigate the incident, and has engaged an independent third-party cybersecurity expert to support the investigation. Cvent has also notified and is actively working with law enforcement and the payment card brands.

Cvent takes security of consumer information seriously. In addition to identifying the vulnerability, Cvent has also enhanced its monitoring, controls, and employee training to prevent this type of situation from reoccurring in the future.

Beginning on or about June 24, 2019, Cvent will be mailing letters to all potentially affected registrants, in substantially the same form as the letters enclosed at Attachment B, on its own behalf and on behalf of the entities listed in Attachment A to the extent Cvent and/or these entities are required to provide such notice.

Please do not hesitate to contact me if you have any questions regarding this matter. Cvent sincerely regrets that this incident occurred, and is committed to working with companies to address this matter.

Sincerely,

Jason C. Chipman

Enclosures

Attachment A

Boston College

National Research Corporation

Attachment B

Sample notices, including sample notices sent from Cvent customers and from Cvent, as well as samples where security code was and was not potentially accessed

[redacted]

June 24, 2019

E7111-L25-0000138 ••••••••••••••••••••SNGLP
[redacted]

Dear [redacted]:

We are writing to notify you of an incident of potential unauthorized access to the credit/payment card you used to recently register for an event. The privacy and protection of event registrants' information is a matter we take very seriously, and we have worked swiftly to resolve the incident. We deeply regret the inconvenience this may cause, and we recommend that you closely review the information provided in this letter for some steps that you may take to protect yourself against potential misuse of your information.

We were notified by a vendor who facilitates our event registration process of a security incident potentially affecting a limited set of our event(s) attendees. Specifically, the vendor became aware of the potential presence of malicious unauthorized code on our event's registration page. The vendor promptly engaged a leading third-party cybersecurity firm and began investigating to determine whether any registrant information may have been affected. The vendor's investigation determined that a malicious unauthorized party was able to insert unauthorized code into a third-party extension utilized by the vendor's creative team on our event's registration webpage. The unauthorized code may have had access to credit/payment card information submitted into certain event guest registration websites between April 16 and May 30, 2019.

While we will not be able to determine with certainty whether any individual's information was accessed by the unauthorized party, it is a possibility. We assess that the information involved in this incident may have included, at most, your credit/payment card information (e.g., name, card number, expiration date, security code, and billing information). No other information was affected. Note that the investigation determined that registrants who used Internet Explorer to register for the event would not have had their information accessed.

We take the security of your information seriously and appreciate the trust you place in us. We have been working diligently with our vendor to investigate the incident, and they have engaged an independent third-party cybersecurity forensic expert to support our investigation. They have also notified and are actively working with law enforcement and payment card brands.

Our vendor has identified the vulnerability, and the situation has been resolved. We have also confirmed that the vendor has enhanced its monitoring, controls, and employee training to prevent this type of situation from reoccurring in the future.

To help protect your identity, to the extent available in your jurisdiction, you are also being offered a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **September 30, 2019** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website: https://www.experianidworks.com/plus
- Provide your **activation code**: [redacted]

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 [redacted] by **September 30, 2019**. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

While we cannot confirm that your data was compromised and used maliciously, you should remain vigilant for incidents of fraud, identity theft, and errors by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported.

Additional details regarding your 12-month Experian IdentityWorks membership and additional steps you can take based on your country and/or state of residency is enclosed.

For More Information

Again, we apologize for any inconvenience caused by this incident. If you have any questions regarding this incident or if you desire further information or assistance, we have set up a call center to provide support. Please do not hesitate to contact us at [redacted] if you have any questions or concerns.

IF YOU ARE A UNITED STATES RESIDENT:

Monitor Your Accounts

You are encouraged to contact the Federal Trade Commission (FTC), law enforcement, or your state attorney general to report incidents of suspected identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.identitytheft.gov

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps, among others: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

Obtain Your Credit Reports

You should also monitor your credit reports. You may periodically obtain credit reports from each nationwide consumer reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

Place a Fraud Alert or Security Freeze on Your Credit File

In addition, you may obtain information from the FTC and the consumer reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide consumer reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last one year. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

Also, you can contact the nationwide consumer reporting agencies regarding if and how you may place a security freeze on your credit report. A security freeze prohibits a consumer reporting agency from releasing information from your credit report without your prior written authorization, which makes it

more difficult for unauthorized parties to open new accounts in your name. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

You may contact the nationwide consumer reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
(800) 349-9960	(888) 397-3742	(888) 909-8872
www.equifax.com	www.experian.com	www.transunion.com

IF YOU ARE AN IOWA RESIDENT:
You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Iowa Attorney General
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5926 / (888) 777-4590
www.iowaattorneygeneral.gov

IF YOU ARE A MARYLAND RESIDENT:
You may obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

IF YOU ARE A NEW MEXICO RESIDENT:
You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov. In addition, New Mexico consumers have the right to submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft.

IF YOU ARE A NORTH CAROLINA RESIDENT:
You may obtain information about preventing identity theft from the North Carolina Attorney

General's Office. This office can be reached at:

North Carolina Department of Justice
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
www.ncdoj.gov

IF YOU ARE AN OREGON RESIDENT:
You may report suspected identity theft to and obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 378-4400
www.doj.state.or.us

IF YOU ARE AN EU RESIDENT:

As a general practice, we recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. You should also review bank account and credit and debit card account statements periodically for unusual activity. If you see anything you do not recognize, you should immediately notify the financial institution as well as the proper law enforcement authorities.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

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

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only. Offline members will be eligible to call for additional reports quarterly after enrolling.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers. The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at [redacted]. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this 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 at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Cvent, Inc.
PO Box 589
Claysburg, PA 16625-0589

June 24, 2019

Dear Sample A Sample:

We are Cvent, a vendor who facilitated [redacted] event registration process. We are writing to notify you of an incident of potential unauthorized access to the credit/payment card you used to recently register for [redacted]. The privacy and protection of event registrants' information is a matter we take very seriously, and we have worked swiftly to resolve the incident. We deeply regret the inconvenience this may cause, and we recommend that you closely review the information provided in this letter for some steps that you may take to protect yourself against potential misuse of your information.

We became aware of the potential presence of malicious unauthorized code on the event registration page that affected a limited set of the event's registrants. We promptly engaged a leading third-party cybersecurity firm and began investigating to determine whether any registrant information may have been affected. The investigation determined that a malicious unauthorized party was able to insert unauthorized code into a third-party extension used on the event's registration webpage. The unauthorized code may have had access to credit/payment card information submitted into the event registration website between April 16 and May 30, 2019.

While we will not be able to determine with certainty whether any individual's information was accessed by the unauthorized party, it is a possibility. We assess that the information involved in this incident may have included, at most, your credit/payment card information (e.g., name, card number, expiration date, and billing information). No other information was affected. Note that the investigation determined that registrants who used Internet Explorer to register for the event would not have had their information accessed.

Working with our independent third-party cybersecurity forensic expert, we identified the vulnerability, and the situation has been resolved. To address the issue, we have also enhanced our monitoring, controls, and employee training to prevent this type of situation from reoccurring in the future. Further, we have also notified and are actively working with law enforcement and payment card brands.

To help protect your identity, to the extent available in your jurisdiction, we are offering you a complimentary one-year membership of Experian's® IdentityWorks^{SM}. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **September 30, 2019** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website: https://www.experianidworks.com/plus
- Provide your **activation code**: **ABCDEFGHI**

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 [redacted] by **September 30, 2019**. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

While we cannot confirm that your data was compromised and used maliciously, you should remain vigilant for incidents of fraud, identity theft, and errors by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported.

Additional details regarding your 12-month Experian IdentityWorks membership and additional steps you can take based on your country and/or state of residency is enclosed.

For More Information

Again, we apologize for any inconvenience caused by this incident. If you have any questions regarding this incident or if you desire further information or assistance, we have set up a call center to provide support. Please do not hesitate to contact us at [redacted] if you have any questions or concerns.

IF YOU ARE A UNITED STATES RESIDENT:

Monitor Your Accounts

You are encouraged to contact the Federal Trade Commission (FTC), law enforcement, or your state attorney general to report incidents of suspected identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.identitytheft.gov

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps, among others: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

Obtain Your Credit Reports

You should also monitor your credit reports. You may periodically obtain credit reports from each nationwide consumer reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

Place a Fraud Alert or Security Freeze on Your Credit File

In addition, you may obtain information from the FTC and the consumer reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide consumer reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last one year. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

Also, you can contact the nationwide consumer reporting agencies regarding if and how you may place a security freeze on your credit report. A security freeze prohibits a consumer reporting agency from releasing information from your credit report without your prior written authorization, which makes it

more difficult for unauthorized parties to open new accounts in your name. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

You may contact the nationwide consumer reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
(800) 349-9960	(888) 397-3742	(888) 909-8872
www.equifax.com	www.experian.com	www.transunion.com

IF YOU ARE AN IOWA RESIDENT:
You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Iowa Attorney General
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5926 / (888) 777-4590
www.iowaattorneygeneral.gov

IF YOU ARE A MARYLAND RESIDENT:
You may obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

IF YOU ARE A NEW MEXICO RESIDENT:
You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov. In addition, New Mexico consumers have the right to submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft.

IF YOU ARE A NORTH CAROLINA RESIDENT:
You may obtain information about preventing identity theft from the North Carolina Attorney

General's Office. This office can be reached at:

North Carolina Department of Justice
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
www.ncdoj.gov

IF YOU ARE AN OREGON RESIDENT:
You may report suspected identity theft to and obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 378-4400
www.doj.state.or.us

IF YOU ARE AN EU RESIDENT:

As a general practice, we recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. You should also review bank account and credit and debit card account statements periodically for unusual activity. If you see anything you do not recognize, you should immediately notify the financial institution as well as the proper law enforcement authorities.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

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

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only. Offline members will be eligible to call for additional reports quarterly after enrolling.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers. The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at [redacted]. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this 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 at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.