MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Jeffrey J. Boogay
Office: (267) 930-4784
Fax: (267) 930-4771
Email: jboogay@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

July 7, 2025

VIA U.S. MAIL

Washington State Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Re: Courtesy Notice of Potential Data Event

To Whom It May Concern:

We represent EventConnect, located at 304 Talbot Street London, ON, N6A 2R4, and are providing a courtesy notice to your office regarding a recent event involving Washington residents. By providing this courtesy notice, EventConnect does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Potential Data Event

On or about May 30, 2025, EventConnect became aware of suspicious activity on their platform. EventConnect quickly took steps to secure the platform, deployed additional security measures and began working with external forensic specialists to investigate the suspicious activity. This investigation determined that between May 28, 2025, and June 2, 2025, an unauthorized party was able to gain access and acquire a small percentage of data relating to specific hotel reservation lists. Within this data, accessible information includes their name, address, telephone number and email address. Information related to individuals' payment card, excluding the CVV, may also have been present. EventConnect does not have any definitive evidence that Washington individuals had payment card information impacted but is providing your office with courtesy notice, out of an abundance of caution.

Notice to Washington Residents

On or about July 7, 2025, EventConnect provided written notice of this incident to impacted Washington residents. Written notice is provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, EventConnect moved quickly to investigate and respond to the suspicious activity, assess the security of EventConnect systems, and identify potentially impacted individuals. Out of an abundance of caution, EventConnect is providing access to credit monitoring services for 24 months, through TransUnion, to individuals whose payment card information may have been accessible, although EventConnect does not have evidence this information was impacted.

Out of an abundance of caution, EventConnect is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. EventConnect is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4784.

Very truly yours,

Jeffrey J. Boogay of
MULLEN COUGHLIN LLC

JJB/lcf
Enclosure

EXHIBIT A

EventConnect
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

July 3, 2025

Notice of Security Incident

Dear

We are writing to inform you of an IT security incident that may have impacted limited personal information belonging to you. We are providing this notice out of an abundance of caution as we are unaware of any identity theft, misuse or fraud in relation to the incident.

What Happened?

On May 30, 2025, we became aware of suspicious activity on our platform. We quickly took steps to secure the platform and deployed additional security measures to prevent similar attacks from occurring in the future. This means that our systems are safe to use.

We also began working with external forensic IT specialists and, with their support, we carried out an extensive investigation into this matter to understand exactly what happened, and how. The investigation determined that, between May 28, 2025, and June 2, 2025, an unauthorized party was able to gain access and acquired a small percentage of the data on our system relating to certain specific hotel reservation lists.

What Information was involved?

The personal information affected consists of your contact information. We are not able to exclude the possibility that some of the accessible reservation lists included payment card details, which means your payment card number and expiry date (no CVV) may have been accessible and are notifying you out of an abundance of caution. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your payment card account statements and to contact your card issuer if you identify any fraudulent charges. As a courtesy, we will be offering two years of complimentary credit monitoring and identity theft protection to impacted individuals through Cyberscout, a TransUnion company.

Response and Steps Taken to Date to Protect You

As soon as we learned of the incident, we quickly identified the threat and took our systems offline. We deployed additional security measures to protect the platform. There has been no suspicious activity on the platform since.

Credit and Identity Theft Monitoring

As noted above, we will provide you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services:

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Should you have any questions related to this incident, or require technical support, representatives are available for 90 days from the date of this letter. To reach the call center, please call **1-833-294-7157.** The call center is available Monday to Friday, from 8:00 am ET to 8:00 pm ET, excluding holidays. Thank you for your understanding, and please do not hesitate to contact us if you have any questions or concerns.

Additional Steps

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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. We encourage consumers to review their 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.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 55 Rhode Island residents that may be impacted by this event.

Should you have additional questions or concerns, please contact security@eventconnect.io.

Sincerely,

John D'Orsay
CEO
EventConnect