

---

Hi,

Below are the details required of a security breach that potentially impacted a resident in your state. Please let us know if you need anything else.

**Number of affected individuals – 1**

**Description of Breach** - On July 24, 2023, an unauthorized user purporting to be a member of our IT Department gained access to our computer network and one of our employees' email accounts. Upon learning that the access was unauthorized, the connection was terminated within approximately 5 minutes of the breach. We immediately involved our IT Department to investigate the scope of the breach and to ensure that our systems were secure. It is our understanding that during the perpetrator's unauthorized access, your credit card information and/or identification card may have been viewed by the unauthorized user. Although we have no information that your sensitive data has been misused in any manner, we are taking appropriate precautionary measures to protect your financial security and to help alleviate concerns you may have.

**Steps Taken in Response** - With the help of our IT consultants, the following steps have been taken: (1) new procedures and policies have been implemented to prevent unauthorized access; (2) all passwords have been changed; (3) a two-step authentication process has been implemented for online system access; and (4) all network firewalls, computers and security protections are confirmed to be properly functioning. We will continue to work with our IT consultants to keep our network and clients safe from a future security breach.

**Crystal Dunn**

Corporate Director of Operations

FCM Hotels, Inc

(c) 919-390-5616

[cdunn@fcmhotels.net](mailto:cdunn@fcmhotels.net)

## **NOTICE OF DATA BREACH**

Dear [Recipient's Name],

I am writing to provide you with a formal notification regarding a data incident involving the computer network at Holiday Inn Express & Suites Culpeper. Although we have no information that your personal information has been misused in any manner, this letter serves to provide additional information concerning the incident, what is being done to correct it, and what you can do to further protect your information.

### **What Happened?**

On July 24, 2023, an unauthorized user purporting to be a member of our IT Department gained access to our computer network and one of our employees' email accounts. Upon learning that the access was unauthorized, the connection was terminated within approximately 5 minutes of the breach. We immediately involved our IT Department to investigate the scope of the breach and to ensure that our systems were secure. It is our understanding that during the perpetrator's unauthorized access, your credit card information and/or identification card may have been viewed by the unauthorized user. Although we have no information that your sensitive data has been misused in any manner, we are taking appropriate precautionary measures to protect your financial security and to help alleviate concerns you may have.

### **What Information Was Involved?**

If you are an individual, all information that was sent or received in an email to Holiday Inn Express & Suites Culpeper, which may have included your name, address, driver's license information, State identification card information, date of birth, telephone number(s), and credit or debit card information.

### **What We Are Doing:**

With the help of our IT consultants, the following steps have been taken: (1) new procedures and policies have been implemented to prevent unauthorized access; (2) all passwords have been changed; (3) a two-step authentication process has been implemented for online system access; and (4) all network firewalls, computers and security protections are confirmed to be properly functioning. We will continue to work with our IT consultants to keep our network and clients safe from a future security breach.

## What You Can Do:

- We strongly recommend you be vigilant in reviewing your bank accounts and brokerage statements, as well as free credit reports.
- We suggest you change any bank account numbers provided to us, and/or have a conversation with your bank regarding the monitoring they can provide. It is also recommended that you change your passwords on all accounts, bank and brokerage.
- We recommend you use one of the three major credit agencies below to place a 90-day fraud alert on your accounts. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts.

|                                                                                                                                                                                                                                                         |                                                                                                                                                                                  |                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Equifax</b><br>P.O. Box 105069<br>Atlanta, GA 30348<br>1-800-525-6285<br><br><a href="https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/">https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/</a> | <b>Experian</b><br>P.O. Box 2002<br>Allen, TX 75013<br>1-888-397-3742<br><br><a href="https://www.experian.com/fraud/center.html">https://www.experian.com/fraud/center.html</a> | <b>TransUnion</b><br>P.O. Box 2000<br>Chester, PA 19016<br>1-800-680-7289<br><br><a href="https://fraud.transunion.com/fa/fraudAlert/landingPage.jsp">https://fraud.transunion.com/fa/fraudAlert/landingPage.jsp</a> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

- You may also want to consider contacting these three credit agencies at the telephone numbers above to place a credit freeze on your credit file. A credit freeze means potential creditors cannot get your credit report, making it less likely that an identify thief can open new accounts in your name. The cost to place and lift a freeze depends on state law. Find your State Attorney General's Office at [naag.org](http://naag.org) to learn more.
- You are also entitled to a free credit report every year from each of these three agencies at [www.annualcreditreport.com](http://www.annualcreditreport.com).
- We also suggest you contact the IRS about getting an Identity Protection PIN to use with your Social Security Number for heightened security. You can do this by going to <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.
- If you suspect identity theft, report it to law enforcement, including the Federal Trade Commission at <https://www.identitytheft.gov/#/> and the State Attorney General's Office at [naag.org](http://naag.org).
- You can obtain more information from the Federal Trade Commission about fraud alerts and security freezes. The Federal Trade Commission can be contacted as follows:

- **Federal Trade Commission**  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-202-326-2222  
<https://www.consumer.ftc.gov/>

The protection and privacy of our clients' information has always been a top priority for our company. We extend our deepest apologies for any inconvenience this incident may have caused you.

**For More Information:**

We are committed to helping those people who may have been impacted by this unfortunate situation. Protecting your information is incredibly important to us, as is addressing this incident with the information and assistance you may need. If you have any questions or concerns, call Seretha Powell, at (252) 557-1406, or email at [spowell@fcmhotels.net](mailto:spowell@fcmhotels.net) or write 787 Madison Road, Culpeper, VA 22701

Sincerely,

Seretha Powell  
Holiday Inn Express & Suites Culpeper