MESSAGE FROM GLOBAL PRESIDENT OF OPERATIONS

Hyatt completes payment card incident investigation

Dear Hyatt Guest,

Protecting customer information is critically important to Hyatt. We have been working tirelessly to complete our previously announced investigation regarding malware that targeted payment card data used at Hyatt-managed locations. We now have more complete information we want to share so that you can take steps to protect yourself.

The investigation identified signs of unauthorized access to payment card data from cards used onsite at certain Hyatt-managed locations, primarily at restaurants, between August 13, 2015 and December 8, 2015. A small percentage of the at-risk cards were used at spas, golf shops, parking, and a limited number of front desks, or provided to a sales office during this time period. The at-risk window for a limited number of locations began on or shortly after July 30, 2015.

The malware was designed to collect payment card data – cardholder name, card number, expiration date and internal verification code – from cards used onsite as the data was being routed through affected payment processing systems. There is no indication that other customer information was affected.

The list of affected Hyatt locations and respective at-risk dates is available at www.hyatt.com/protectingourcustomers. Additionally, for at-risk transactions where a cardholder's name was affected, we are in the process of mailing letters to customers for whom we have a mailing address and sending emails to customers for whom we only have an email address.

We worked quickly with leading third-party cyber security experts to resolve the issue and strengthen the security of our systems in order to help prevent this from happening in the future. We also notified law enforcement and the payment card networks. Please be assured that you can confidently use payment cards at Hyatt hotels worldwide.

Most importantly, we encourage you to remain vigilant and to review your payment card account statements closely. You should report any unauthorized charges to your card issuer immediately. Speak to your card issuer for details because, while card issuers' policies related to fraud may vary, payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner.

Additionally, Hyatt has arranged for CSID to provide one year of CSID's Protector services to affected customers at no cost to them. CSID is one of the leading providers of fraud detection solutions and technologies. In order to activate CSID's Protector coverage, affected customers in the U.S. may visit www.csid.com/hyatt-us and affected customers outside the U.S. may visit www.csid.com/hyatt-intl to complete a secure sign up and enrollment process.

If you have questions or would like more information, please call 1-877-218-3036 (U.S. and Canada) or +1-814-201-3665 (International) from 7 a.m. to 9 p.m. EST.

Please be assured that we take the security of customer data very seriously. We deeply regret the inconvenience and any concern this may have caused you.

Sincerely,

Chuck Floyd
Global President of Operations
Hyatt Hotels Corporation

Frequently Asked Questions

What happened?
In late November, Hyatt identified malware on computers that operate the payment processing systems for Hyatt-managed locations. The company immediately launched an investigation and engaged leading third-party cyber security experts. The investigation identified signs of unauthorized access to payment card data from cards used onsite at certain Hyatt-managed locations, primarily at restaurants, between August 13, 2015 and December 8, 2015. A small percentage of the at-risk cards were used at spas, golf shops, parking, and a limited number of front desks, or provided to a sales office during this time period. The at-risk window for a limited number of locations began on or shortly after July 30, 2015. Hyatt worked quickly with leading third-party cyber security experts to resolve the issue and strengthen the security of its systems, and customers can confidently use payment cards at Hyatt hotels worldwide.

What type of information is affected?
The malware was designed to collect payment card data – cardholder name, card number, expiration date and internal verification code – from cards used onsite as the data was being routed through affected payment processing systems. There is no indication that other customer information was affected.

Is my payment card information affected?
It is possible that any payment card used onsite at certain Hyatt-managed locations, primarily at restaurants, between August 13, 2015 and December 8, 2015. A small percentage of the at-risk cards were used at spas, golf shops, parking, and a limited number of front desks, or provided to a sales office during this time period. The at-risk window for a limited number of locations began on or shortly after July 30, 2015. The list of affected Hyatt locations and respective at-risk dates is available at www.hyatt.com/protectingourcustomers.

Please refer to your account statements to see if you used a card at an affected location during a relevant time period. If you believe your payment card was affected or you see any unusual activity on your account statement, you should contact your card issuer immediately.

Did you notify affected customers directly?
For at-risk transactions where a cardholder's name was affected, we are in the process of mailing letters to customers for whom we have a mailing address and sending emails to customers for whom we only have an email address. However, we do not have sufficient information to be able to identify and contact all potentially affected individuals, which is why we encourage customers to reference the list of affected locations and respective at-risk dates.

Which locations were affected?
The list of affected Hyatt locations and respective at-risk dates is available at www.hyatt.com/protectingourcustomers.

Is it safe to use a payment card at Hyatt hotels and resorts?
Customers can confidently use payment cards at Hyatt hotels worldwide. We worked quickly with leading third-party cyber security experts to resolve the issue and strengthen the security of our systems in order to help prevent this from happening in the future.

What actions have you taken to ensure this does not happen again?
We have been working with leading third-party cyber security experts to ensure that this issue has been fully addressed and implement additional security measures to strengthen the security of our systems.

How can customers protect themselves?
We encourage all customers to review their payment card account statements closely and to report any unauthorized charges to their card issuers immediately. Speak to your card issuer for details because, while

card issuers' policies related to fraud may vary, payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner.

Additionally, Hyatt has arranged for CSID to provide one year of CSID's Protector services to affected customers at no cost to them. CSID is one of the leading providers of fraud detection solutions and technologies. In order to activate CSID Protector coverage, affected customers in the U.S. may visit www.csid.com/hyatt-us and customers outside the U.S. may visit www.csid.com/hyatt-intl to complete a secure sign up and enrollment process.

How do I find out more information?
If you have questions or would like more information, please call 1-877-218-3036 (U.S. and Canada) or +1-814-201-3665 (International) from 7 a.m. to 9 p.m. EST.

What can I do if my card might be affected?
We encourage you to monitor your payment card account statements for unauthorized activity. You should report any unauthorized charges to your card issuer immediately. The phone number to call is usually on the back of the card. Speak to your card issuer for details because, while card issuers' policies related to fraud may vary, payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner.

Could I still experience fraud after December 8, 2015?
While customers can confidently use payment cards at Hyatt hotels worldwide, any payment card that was used onsite at an affected location during the respective at-risk dates could still be subject to fraud even if you have not yet seen fraudulent activity. We are continuing to work closely with payment card companies to identify potentially affected cards so that the banks that issued those cards can be made aware and initiate heightened monitoring of those cards.

Are you working with government authorities?
We have notified the appropriate country and state regulators. We are also working with the U.S. Federal Bureau of Investigation.