goulston&storrs
counsellors at law

Christian W. Habersaat
chabersaat@goulstonstorrs.com
(617) 574-3549 (tel)
(617) 574-7529 (fax)

July 17, 2017

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

Re: Nantucket Island Resorts LLC

Dear Sir/Madam:

We represent Nantucket Island Resorts LLC ("NIR"). We are writing to notify you of a data security incident that potentially compromised the security of personal information of one (1) New Hampshire resident who made a hotel reservation at a hotel and marina owned and managed by NIR using a reservation system operated, managed and controlled by NIR's vendor, Sabre Inc. ("Sabre"). NIR's investigation into the event described below is ongoing, and this notice will be supplemented to the extent that any additional material information is learned.

Nature of Data Security Event

NIR owns and manages several vacation properties in Nantucket, Massachusetts. NIR contracts with Sabre for access to SynXis Central Reservations system, Sabre's web-based reservation platform, which allows consumers to make vacation bookings on sites like Expedia at a multitude of hotels including the properties owned by NIR.

On June 7, 2017, Sabre notified NIR concerning unusual activity on an account involving access to hotel reservation data. A copy of Sabre's notification letter is attached hereto. Specifically, Sabre alerted NIR that an unauthorized party obtained access to a subset of hotel reservations processed through Sabre's reservation system, including reservations for the properties owned by NIR. NIR understands that the information potentially accessed by the unauthorized party included guest names, addresses, phone numbers, e-mails, payment card numbers, cardholder's names, card expiration dates, and for a subset of reservations, payment card security codes. NIR understands that the unauthorized party first obtained access on August 10, 2016 and last accessed the information on March 9, 2017.

Sabre indicated that it had engaged Mandiant, a leading cybersecurity firm, to investigate the incident, and represented to NIR that it took successful measures to ensure that the

unauthorized access to the SynXis Central Reservations system is no longer possible. Sabre also represented that it had notified law enforcement and major payment card brands about this incident. Furthermore, Sabre has engaged Epiq Systems to work with hotels on notifying affected consumers of the data breach.

NIR has no control over SynXis Central Reservations system and is not privy to the investigative analysis into the reported breach conducted by or on behalf of Sabre. Based on the press and other reports, NIR understands that this incident likely affected thousands of hotel properties owned and managed by other companies. According to the investigation conducted by NIR, there is no indication of exposure or unauthorized access to any system controlled by NIR. Likewise, NIR is not aware of, and has not received any reports or complaints of, the misuse of the personal information that was submitted by its guests on Sabre's reservation system.

Sabre provided NIR with a list of guests affected by this breach and further advised NIR that the unauthorized access was limited to the individuals identified by Sabre on this list. NIR has begun the process of conveying this information to Epiq who in turn will be notifying such guests of the reported incident. The guests will be informed that NIR recently learned about the unauthorized access to the guests' personal information and that steps should be taken to be alert to signs of any misuse of such information. These persons will also be advised of their right to obtain a police report, how to request a security freeze and the ability to obtain credit reports from any of the credit reporting agencies. NIR will monitor Epiq's notification process.

In short, NIR will continue to investigate this reported incident, monitor the guest notification process, and will advise your office if any new significant information is learned. We are, or course, available to discuss this matter with you, if you wish, at your convenience.

Very truly yours,

Christian W. Habersaat

CWH:vmm
Enclosure

Sabre

June 6, 2017

Dear Valued Sabre Partner:

We are writing to update you on the previously disclosed incident involving unauthorized access to payment card information in a subset of hotel reservations made through the Sabre Hospitality Solutions SynXis Central Reservations system (CRS). The unauthorized activity only affected a subset of reservations processed through the CRS. Not all users of the CRS were impacted. Unfortunately, reservations related to your business were affected.

This letter will cover the details of the incident, the findings of our investigation, and how we are prepared to further assist you.

What Happened?
Sabre launched an investigation into unusual activity on an account involving access to hotel reservation data. The investigation was supported by third party experts, including Mandiant, a leading cybersecurity firm. Our investigation determined that an unauthorized party:

- obtained access to account credentials that permitted access to a subset of hotel reservations processed through the CRS;
- used the account credentials to view a credit card summary page on the CRS and access payment card information (although we use encryption, this credential had the right to see unencrypted card data); and
- first obtained access to payment card information and some other reservation information on August 10, 2016. The last access to payment card information was on March 9, 2017.

Our investigation did not uncover forensic evidence that the unauthorized party removed any information from the system, but it is a possibility.

We took successful measures to ensure this unauthorized access to the CRS was stopped and is no longer possible. There is also no indication that any other Sabre systems beyond the CRS, such as Sabre's Airline Solutions and Travel Network platforms, were affected or accessed by the unauthorized party.

What Information Was Involved?
The unauthorized party was able to access information for certain hotel reservations, including cardholder name; payment card number; card expiration date; and, for a subset of reservations, card security code. The unauthorized party was also able, in some cases, to access certain information such as guest name(s), email, phone number, address, and other information if provided to the CRS. Information such as Social Security, passport, or driver's license number was not accessed. A list of data fields and an explanation of the fields is included as Attachment A; however, for many reservations, a number of these fields may have contained no data.

Because we purge payment card information 60 days after guest departure dates, we no longer have the payment card data for approximately half of the affected reservations. In addition, for a large percentage of bookings, payment card security codes were never provided to the CRS as part of the reservation and would not have been accessible to the unauthorized party. To the extent the CRS was provided with a payment card security code, the code was purged from the CRS within 24 hours of the creation of the payment record. We also note that certain customers and partners use virtual cards or other payment methods such that the payment card information may not reflect a guest payment card.

We have created a file with information about your affected reservations that is available for you to download concurrently with this letter. Note that for security reasons the file does not contain full payment card numbers. The card brands have been provided with a file containing those full payment card numbers related to this matter that are still present on the CRS.

What We Are Doing and What You Can Do
We notified law enforcement and the payment card brands, and we engaged a PCI Forensic Investigator to investigate this incident.

Sabre is committed to a global, holistic security program focused on protecting our systems. In fact, our level of investment in state of the art security technology and highly qualified personnel has more than tripled since 2013. Using a layered security approach, we have enhanced the security around our access credentials and the monitoring of system activity to further detect and prevent unauthorized access. Consistent with that approach, we enlist best-in-class external resources to reassure you that Sabre addresses security with the utmost care and expertise.

Some U.S. and non-U.S. jurisdictions may have laws that require disclosure of certain data security incidents to affected consumers and government regulators. We have worked to provide tools and resources to support you. As such, information is enclosed about the following:

- **Complimentary notice support**: If you would like assistance with providing notice to affected consumers, Sabre has engaged Epiq Systems to provide certain services at no cost to you. These services include direct mail or email to affected consumers and a call center. This is an optional service that is available, and full details are enclosed as Attachment B.
- **Sample notice letter**: A sample notification letter is enclosed as Attachment C, which you may choose to adapt to any requirements of applicable jurisdiction(s) and send to your customers notifying them of this incident.
- **Website**: A microsite is available to link from your website if you find it is a helpful resource in providing notice to your customers. The text of the microsite is enclosed as Attachment D.
- **FAQ**: A list of anticipated questions and answers is enclosed as Attachment E.

For More Information
On behalf of the entire Sabre team, we sincerely regret that this incident occurred. Your business is extremely important to us and we value the trust you place in us by choosing Sabre. We appreciate the support and collaboration so many of you, our customers and partners, have demonstrated throughout this matter. Our industry, like many, faces ever increasing cybersecurity threats that require strong partnerships across the travel ecosystem in response. Sabre is proud to be your partner in combating this challenge and ensuring your guests are protected.

Should you have any questions, please contact your account manager or call 877-367-2269 toll-free from the U.S. or Canada, or you can call one of our global support numbers available at http://sabrehospitality.com/contact.

Sincerely,

Sean Menke
President and CEO

ATTACHMENT A: List of Fields

In conjunction with this letter, you received a link to download a file containing information about your affected reservations. Please review the chart below to understand the contents of this file. The file is in "comma separated value" (.csv) format.

Of the data fields listed below, the unauthorized party potentially viewed only the information indicated below with an asterisk. We are providing additional fields in case they would be helpful in locating records in your system. Many fields in your file may be blank and contain no information. In some instances, the information may not have been provided to the CRS at the time of booking. In others, the information may have been purged from the CRS. The CRS purges all credit card information 60 days after guest departure. If a payment card security code is entered into the CRS, it is purged within 24 hours.

In some cases, opening the spreadsheet directly in Excel will prevent certain characters (i.e., non-English language characters) from displaying properly. Please follow the directions in Attachment F on how to open the file to ensure the information displays correctly.

Field Name	Description
CHAIN_NAME*	The customer-facing name of the hotel chain provided by the hotel in the CRS. If a hotel is not a part of a chain, the hotel name will display in this field.
CHAIN_ID	Unique identification number assigned to the chain by the CRS.
HOTEL_NAME*	Customer-facing name of the hotel where the reservation was made.
HOTEL_ID	Unique identification number assigned to the hotel property by the CRS.
PRI_CHANNEL	Primary booking channel through which reservation was made.
SEC_CHANNEL	The secondary channel is a subset of the primary channel and provides an additional level of detail about where the reservation originated.
SUB_SOURCE_CODE	An additional level of detail about where a booking may have originated from, which is used only in the CRS for certain primary and secondary channel combinations.
CRS_CONFIRM	Unique identification number assigned to the reservation by the CRS.
CHANNEL_CONFIRM	Unique identification number assigned by third-party booking channels to the reservation.
RECORD_LOCATOR	Unique alpha identifier assigned by the GDS to the reservation.
PMS_CONFIRM	Unique identification number assigned to the reservation by the Property Management System (PMS) provider.
REZ_STATUS*	Status of reservation.
BOOK_DATE*	Date when reservation was confirmed in the CRS.
ARRIVAL*	Date of scheduled guest arrival.
DEPART*	Date of scheduled guest departure.
GUEST_FIRST_NAME*	Name, if provided at booking by Guest. **Note for Guest fields**: Primary guest name and information is provided for each reservation, unless the only payment card associated with the reservation belongs to a secondary guest. Secondary guest information is provided only where a payment card is associated with that Guest.
GUEST_LAST_NAME*	Name, if provided at booking by Guest.
GUEST_EMAIL*	Email address, if provided at booking by Guest.
GUEST_ADDR1*	Street address, if provided at booking by Guest.

GUEST_ADDR2*	Additional street address line, if provided at booking by Guest.
GUEST_CITY*	Address city, if provided at booking by Guest.
GUEST_STATE*	Address state, if provided at booking by Guest.
GUEST_ZIP*	Address zip code, if provided at booking by Guest.
GUEST_COUNTRY*	Address, if provided at booking by Guest.
GUEST_PHONE*	Phone number, if provided at booking by Guest.
CARDHOLDER_NAME*	Name on payment card associated with reservation. This information is purged 60 days after Guest departure.
CARD_BRAND*	Brand of payment card associated with reservation. This information is purged 60 days after Guest departure.
CARD_LAST_4*	The last four digits of the payment card associated with the reservation. This information is purged 60 days after Guest departure.
CARD_EXPIRE*	The expiration of the payment card associated with the reservation. This information is purged 60 days after Guest departure.
CARD_CVV*	The security code (such as CVV2) of the payment card associated with the reservation. This information is purged within 24 hours where provided to CRS.
ROOM_TYPE_CODE*	Alpha-numeric code defining the room type of the reservation.
RATE_PLAN_CODE*	Alpha-numeric code defining the rate plan of the reservation.
ADULTS*	Number of adults associated with reservation, as provided by guest at booking.
CHILDREN*	Number of children associated with reservation, as provided by guest at booking.
IATA_NO	Unique travel agency identification number provided by the booking channel.
TA_LEGAL_NAME	Travel Agency legal name provided by the booking channel.
TA_DBA_NAME	Travel Agency "Doing Business As" name provided by the booking channel.

ATTACHMENT B: Complimentary Notice Support

If you determine notice for affected consumers is required, Sabre has engaged Epiq Systems, a leading global provider of integrated technology and legal services, as an optional resource for certain services at no cost to you.

Among the services available to you are:

- Direct mail or email notice to consumers;
- Call center support for consumers who seek additional information;
- A microsite to link from your website that you may wish to consider using as part of providing notice to your customers, if appropriate. The microsite is at www.sabreconsumernotice.com.

To begin the process with Epiq Systems, call 888-721-6306 toll free in the U.S. (Monday through Friday, 9:00am – 9:00pm EDT) or visit www.sabrelodgingnotice.com. In order to properly assess and best understand your needs, Epiq will need the following information from you:

- Company name
- Number of affected reservations
- Point of contact including name, phone number and email address

Following your initial contact, Epiq will route your specific details to an account representative who will respond to discuss next steps.

ATTACHMENT C: Sample Notification Letter

A sample notification letter for U.S. consumers is below, which you may choose to adapt to any requirements of applicable jurisdiction(s) and send to your customers notifying them of this incident. ***Notice obligations vary by jurisdiction.*** *The letter may also need to be adapted to reflect the information you provided to the CRS. For example, if you did not provide payment card security codes to the CRS, then they would not have been accessed by the unauthorized party.*

[NAME AND ADDRESS OF COMPANY PROVIDING NOTICE]

[DATE]

[CUSTOMER NAME AND ADDRESS]

NOTICE OF DATA BREACH

Dear Valued Customer:

We are writing to you because of an incident involving unauthorized access to customer information associated with your hotel reservation(s). The privacy and protection of our customers' information is a matter we take very seriously, 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.

What Happened?

The Sabre Hospitality Solutions SynXis Central Reservations system (CRS) facilitates the booking of hotel reservations made by consumers through hotels, online travel agencies, and similar booking services. Following an examination of forensic evidence, Sabre notified us on or about June 6, 2017 that an unauthorized party gained access to account credentials that permitted unauthorized access to unencrypted payment card information, as well as certain reservation information, for a subset of hotel reservations processed through the CRS.

The investigation determined that the unauthorized party first obtained access to payment card and other reservation information on August 10, 2016. The last access to payment card information was on March 9, 2017.

What Information Was Involved?

The unauthorized party was able to access payment card information for your hotel reservation(s), including cardholder name; card number; card expiration date; and, potentially, your card security code. The unauthorized party was also able, in some cases, to access certain information such as guest name, email, phone number, address, and other information. Information such as Social Security, passport, or driver's license number was not accessed.

What We Are Doing

Sabre engaged a leading cybersecurity firm to support its investigation. Sabre also notified law enforcement and the payment card brands about this incident.

What You Can Do

You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized activity. 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.

In addition, you may contact the Federal Trade Commission (FTC) or law enforcement, such as your state attorney general, to report incidents of 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)
https://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: (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 Report

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

Place a Fraud Alert or Security Freeze on Your Credit Report File

In addition, you may obtain information from the FTC and the credit 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 credit 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 90 days. 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 credit reporting agencies regarding if and how you may place a security freeze on your credit report. A security freeze prohibits a credit 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. The credit reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. You may be charged to place or lift a security freeze. 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 credit reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
(800) 525-6285	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

Please see the following page for certain state-specific information.

For More Information

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, please do not hesitate to contact us at [TELEPHONE NUMBER (toll-free, if available) OF PERSON OR BUSINESS REPORTING THE BREACH].

Sincerely,

[SIGNATURE]

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

Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
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 Obtain a Security Freeze or Submit a Declaration of Removal

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. the unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. proper identification to verify your identity;
3. information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and
4. payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies using the contact information provided in the enclosed letter.

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
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.gov

IF YOU ARE AN OREGON RESIDENT:
You may 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
http://www.doj.state.or.us/

ATTACHMENT D: Consumer-Facing Microsite Text

A microsite is available to link from your website that you may wish to consider using as part of providing substitute notice to your customers, if appropriate. The working text is as follows:

[DATE]

NOTICE OF DATA BREACH

You have been directed to this site because a hotel reservation you booked may have been impacted by a data incident. This incident may affect consumers whose payment cards were used to book reservations through the company that directed you to this website.

The data incident occurred at Sabre Hospitality Solutions, a company that offers reservation systems and other services to hotels, online travel agencies, and booking services, including the one that directed you to this site. The privacy and protection of consumers' information is a matter we take very seriously, and we recommend that you closely review the information provided below for some steps that you may take to protect yourself against potential misuse of your information.

What Happened?

The Sabre Hospitality Solutions SynXis Central Reservation System (CRS) facilitates the booking of hotel reservations made by consumers through hotels, online travel agencies, and similar booking services. Following an examination of forensic evidence, Sabre notified us on or about June 6, 2017 that an unauthorized party gained access to account credentials that permitted unauthorized access to payment card information, as well as certain reservation information, for a subset of hotel reservations processed through the CRS.

The investigation determined that the unauthorized party first obtained access to payment card and other reservation information on August 10, 2016. The last access to payment card information was on March 9, 2017.

This incident may affect some consumers whose payment cards were used to book reservations through the company that directed you to this website.

What Information Was Involved?

The unauthorized party was able to access payment card information for hotel reservations, including cardholder name; payment card number; card expiration date; and, for a subset of reservations, payment card security code. The unauthorized party was also able, in some cases, to access certain information such as guest name, email, phone number, address, and other information. Information such as Social Security, passport, or driver's license number, was not accessed.

What We Are Doing

The data incident occurred at Sabre Hospitality Solutions. Sabre engaged a leading independent cybersecurity firm to support the investigation and notified law enforcement and the payment card brands about this incident. There is no evidence of continued unauthorized activity.

Sabre is committed to a global, holistic security program focused on protecting its systems and your information. Using a layered security approach, and as part of its ongoing efforts to consistently improve

security based on evolving threats and security best practices, Sabre has enhanced the security around its access credentials and the monitoring of system activity to further detect and prevent unauthorized access.

What You Can Do

You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized activity. 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.

In addition, you may contact the Federal Trade Commission (FTC) or law enforcement, such as your state attorney general, to report incidents of 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)
https://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: (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 Report

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

Place a Fraud Alert or Security Freeze on Your Credit Report File

In addition, you may obtain information from the FTC and the credit 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 credit 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 90 days. 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 credit reporting agencies regarding if and how you may place a security freeze on your credit report. A security freeze prohibits a credit 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. The credit reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. You may be charged to place or lift a security freeze. 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 credit reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
(800) 525-6285	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

For More Information

We apologize for any inconvenience caused by this incident. We are working hard to make this right. If you have any questions regarding this incident or if you desire further information or assistance, please contact the company that directed you to this website.

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

Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
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 MASSACHUSETTS RESIDENT:
Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax, Experian, and TransUnion by regular, certified, or overnight mail at the addresses below:

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
(800) 525-6285	(888) 397-3742	(800) 680-7289

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior 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, military identification, etc.);

7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express, or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

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 Obtain a Security Freeze or Submit a Declaration of Removal

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. the unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. proper identification to verify your identity;
3. information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and
4. payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies using the contact information provided above.

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
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.gov

IF YOU ARE AN OREGON RESIDENT:
You may 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
http://www.doj.state.or.us/

IF YOU ARE A RHODE ISLAND RESIDENT:
You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at:

RI Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
http://www.riag.ri.gov/

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five (5) business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number or password provided by the consumer reporting agency.
2. Proper identification to verify your identity.
3. The proper information regarding the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of an account review, collection, fraud control, or similar activities.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze -- either completely, if you are shopping around, or specifically for a certain creditor -- with enough advance notice before you apply for new credit for the lifting to take effect.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report.

Unless you are sixty-five (65) years of age or older, or you are a victim of identity theft with an incident report or complaint from a law enforcement agency, a consumer reporting agency has the right to charge you up to ten dollars ($10.00) to place a freeze on your credit report; up to ten dollars ($10.00) to temporarily lift a freeze on your credit report, depending on the circumstances; and up to ten dollars ($10.00) to remove a freeze from your credit report. If you are sixty-five (65) years of age or older or are a victim of identity theft with a valid incident report or complaint, you may not be charged a fee by a consumer reporting agency for placing, temporarily lifting, or removing a freeze.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above.

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Complete address;
5. Prior addresses;
6. Proof(s) of identification (state driver's license or ID card, military identification, birth certificate etc.)
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, payment. Do not send cash through the mail.

ATTACHMENT E: FAQ

DETAILS OF THIS SECURITY INCIDENT

How and when did you discover the issue?
As discussed in our communications to you on May 2, 2017, we were investigating, with the help of expert third parties, an incident involving unauthorized access to payment information contained in a subset of hotel reservations processed through the CRS. We retained the third parties in April 2017.

What prompted the investigation?
The investigation began after we became aware of unusual activity on an account involving access to hotel reservation data.

When was the unauthorized access to payment card information shut off?
The last access to payment card information was on March 9, 2017.

What did the credentials allow access to?
The unauthorized party was able to access payment card numbers and, in some cases, certain information such as guest name, email, phone number, address, and other information if provided to the CRS. Information such as Social Security, passport, or driver's license number was not accessed. A list of data fields is included in Attachment A; however, for many reservations, a number of these fields may have contained no data because the data was purged or never provided to the CRS.

What exactly did the unauthorized party see when accessing the system?
With respect to the data fields provided in Attachment A, the unauthorized party potentially viewed those data fields marked with an asterisk in Attachment A. We are providing additional fields in case they would be helpful in locating records in your system. Many fields in your file may be blank and contain no information. In some instances, the information may not have been provided to the CRS at the time of booking. In others, the information may have been purged from the CRS. The CRS purges all credit card information 60 days after guest departure. If a payment card security code is entered into the CRS, it is purged within 24 hours.

Did compromised credentials give access to other systems?
There is no evidence that any other Sabre systems beyond the CRS, such as Sabre's Airline Solutions and Travel Network platforms, were affected or accessed by the unauthorized party.

Are reservations made through the Sabre-run call center affected?
Our investigation did not indicate that any other of Sabre's systems beyond the CRS were affected or accessed by the unauthorized party.

Can you confirm that my system was not infiltrated or accessed in anyway?
Our investigation did not indicate that the unauthorized party moved from the CRS into any other system.

Does this incident have anything to do with the recent news at IHG?
No, this is unrelated as far as we are aware.

Does this incident have anything to do with recent outages?
No, this is unrelated.

Did you notify law enforcement?

We notified law enforcement and continue to support their investigation.

Have you notified the card brands?
We have notified the major card brands about this incident and have sent them the affected numbers that we still have in the CRS.

INVESTIGATION RESULTS

What did your investigation reveal?
Our investigation, supported by Mandiant, a leading cybersecurity firm, determined that an unauthorized party:

- obtained access to account credentials that permitted access to a subset of hotel reservations processed through the CRS;
- used the account credentials to view a credit card summary page on the CRS and access payment card information (although we use encryption, this credential had the right to see unencrypted card data); and
- first obtained access to payment card information and some other reservation information on August 10, 2016. The last access to payment card information was on March 9, 2017.

Our investigation did not uncover forensic evidence that the unauthorized party removed any information from the system, but it is a possibility.

We took successful measures to ensure this unauthorized access to the CRS was stopped and is no longer possible. There is also no indication that any other Sabre systems beyond the CRS, such as Sabre's Airline Solutions and Travel Network platforms, were affected or accessed by the unauthorized party.

How many reservations were accessed?
We have provided a file with information about your affected reservations that is available for you to download. This information tallies the reservations for your customers and should assist you in locating the reservations in your system. In some cases, the information provided may include addresses for consumers. However, in many cases, the CRS does not receive addresses for the consumers. Please consult your file.

If a guest's data was accessed, does that mean it was definitely removed by the unauthorized party?
Our investigation did not uncover forensic evidence that the unauthorized party removed any information from the CRS, but it is a possibility. For a large percentage of reservations, payment card security codes were never provided to the CRS and accordingly, the security codes would not have been accessible to the unauthorized party. In some cases, reservations were made using virtual payment cards.

Why do you keep the credit card or other payment information for 60 days after guest departure?
Our hotel operators and channel partners may use this information in the event that they need to close out transactions with their consumers after the consumers have departed from the hotel. By keeping payment card information encrypted in the CRS for 60 days, we are able to facilitate this process.

Was the payment card information that was accessed encrypted?
Although we store payment information in the reservation in encrypted form, the unauthorized party was able to access the information in unencrypted format by using a credential that had the right to see unencrypted data.

Why was the payment card information unencrypted?

We store payment information in the CRS in encrypted form. However, payment card information on the credit card summary page is unencrypted so that hotels can access it to process reservations. Such access is highly restricted, but this credential had the right to see unencrypted card data.

SECURITY OF SABRE'S SYSTEMS

How do we know the Sabre systems are secure?
We took successful measures to ensure that the unauthorized access to the CRS was stopped. There is also no indication that any other Sabre systems beyond the CRS were affected or accessed by the unauthorized party. This is based on our internal investigation, as well as the work of independent experts who are advising us.

Is this issue limited to Sabre's CRS? Could other systems have been accessed through the CRS?
There is no indication that any other Sabre systems were affected or accessed beyond the SynXis CRS.

What data is held within the CRS? Does it include guests' payment card information?
The unauthorized party was able to access payment card numbers and, in some cases, certain information such as guest name, email, phone number, address, and other information if provided to the CRS. Information such as Social Security, passport, or driver's license number, was not accessed. A list of data fields is included in Attachment A; however, for many reservations, a number of these fields may have contained no data.

What is Sabre doing to make all of your systems more secure?
Sabre is committed to a global, holistic security program focused on protecting our systems. In fact, our level of investment in state of the art security technology and highly qualified personnel has more than tripled since 2013. Using a layered security approach, we have enhanced the security around our access credentials and the monitoring of system activity to further detect and prevent unauthorized access. Consistent with that approach, we enlist best-in-class external resources to reassure you that Sabre addresses security with the utmost care and expertise.

GUEST/FRANCHISEE COMMUNICATIONS

What notice is required to consumers and regulators?
Some U.S. and non-U.S. jurisdictions may require disclosure of certain data security incidents to affected consumers and government regulators. A sample notification letter for U.S. consumers is included as Attachment C, which you may choose to adapt to any requirements of applicable jurisdiction(s) and send to your customers notifying them of this incident. However, notice obligations vary by jurisdiction. The letter may also need to be adapted to reflect the information you provided to the CRS. For example, if you did not provide payment card security codes to the CRS, then they would not have been accessed by the unauthorized party.

Is Sabre support for notice obligations for the U.S. only, or is it global support?
Epiq is able to provide certain support for applicable notice obligations for U.S. and international consumers, once you determine how you would like to proceed.

Is Sabre notifying consumers?
We are working with all of our impacted customers and providing them with an array of support options should they determine that they need to notify their consumers. If you determine that consumer notification is required, Sabre has engaged Epiq Systems to provide certain services, including direct mail or email support and a call center, at no cost to you. Full details are enclosed as Attachment B.

Are the hotels providing notice? Are the channel partners or online travel agencies providing notice?
We cannot advise you on your legal obligations. We are working with all of our impacted customers to provide them information on their affected reservations and providing them with an array of support options should they determine that they need to notify their consumers.

What are my notice obligations to my guests? What information must I include? Do I still need to notify my guests if my hotel is not the merchant of record?
While we cannot advise you on your legal obligations, some U.S. and non-U.S. jurisdictions may require disclosure of certain data security incidents to affected consumers and government regulators. We have prepared a sample letter, enclosed as Attachment C, which you may choose to adapt and send to your customers notifying them of this incident. Please note, however, that you may need to tailor the template to comply with applicable jurisdictional requirements.

Are you going to email my guests directly or do I have to?
If you determine that consumer notification is required, Sabre has engaged Epiq Systems to provide certain services, including direct mail, email support, and a call center, at no cost to you. Full details are enclosed as Attachment B.

Will Sabre help me understand the different privacy and data laws in various countries around the world? What happens if I don't notify guests?
We cannot advise you on your legal obligations. If you determine that consumer notification is required, Sabre has engaged Epiq Systems to provide certain services, including direct mail, email support, and a call center, at no cost to you. Full details are enclosed as Attachment B.

What if I don't have full contact information for a consumer?
We created a file with information about your affected reservations that is available for you to download. We are not in a position to speak for any of our partners regarding whether they will share consumer contact information that they may have collected regarding your affected reservations. If you determine that consumer notification is required, Sabre has engaged Epiq Systems to provide certain services, including direct mail, email support, and a call center, at no cost to you. Full details are enclosed as Attachment B.

I am a hotel brand, but I don't have address information for all of my affected guests. Can I get the information from Sabre or from the online travel agency or other entity that took the reservation?
While we are not in a position to speak for any of our partners, we created a file with information about your affected reservations that is available for you to download. This file includes consumer contact information if it was provided to, and remains available in, the CRS.

I am a hotel. Will the online travel agencies or channel partners contact my guests?
We are not in a position to speak for any of our OTA partners. You may wish to follow up with OTAs or channel partners regarding these questions.

What will Sabre do to handle the communication to my customers and take responsibility for this?
If you determine that consumer notification is required, Sabre has engaged Epiq Systems to provide certain services, including direct mail, email support, and a call center, at no cost to you. Full details are enclosed as Attachment B.

Do I need to notify my franchisees about this issue? What information should I provide?

While we cannot advise you on your legal obligations, we created a file with information about your affected reservations that is available for you to download.

Someone should notify consumers, but I don't believe it should be me. How can I make sure that someone fulfills this obligation?
We cannot advise you on your legal obligations. We are working with all of our impacted customers and providing them with an array of support options should they determine that they need to notify their consumers. We have created a file with information about your affected reservations that is available for you to download. Further, if you determine that consumer notification is required, Sabre has engaged Epiq Systems to provide certain services at no cost to you. Full details are enclosed as Attachment B. We have also prepared a sample notification letter for U.S. consumers, included as Attachment C, which you may choose to adapt to any requirements of applicable jurisdiction(s) and send to your customers notifying them of this incident.

Can you tell me the number of impacted consumers in any particular state?
We have provided you with a file with information about your affected reservations that is available for you to download. This information should assist you in locating the reservations in your system. In some cases, the information provided may include addresses for consumers. However, in many cases, CRS does not receive addresses for the consumers. Please consult your file.

Were payment card security codes accessed? Can Sabre tell me if it received payment card security codes from me?
Our investigation identified that while some payment card security codes may have been accessed for a subset of reservations, many reservations never provided payment card security codes to the CRS—in which case they would not have been accessible to the unauthorized party, and many others used virtual cards or other payment methods such that the payment card information may not reflect a guest payment card. You may wish to consult your team to determine if you furnish security codes to the CRS as part of the booking process.

If a field is blank in the file you sent me, does that mean Sabre never received info such as payment card number or card security code?
Not necessarily. Because we purge payment card information 60 days after guest departure dates, we no longer have the payment card numbers for approximately half of the affected reservations. In addition, for a large percentage of reservations, payment card security codes were never provided to the CRS as part of the reservation and would not have been accessible to the unauthorized party. To the extent we were provided with a card security code, the code was purged from the CRS within 24 hours of the creation of the payment record.

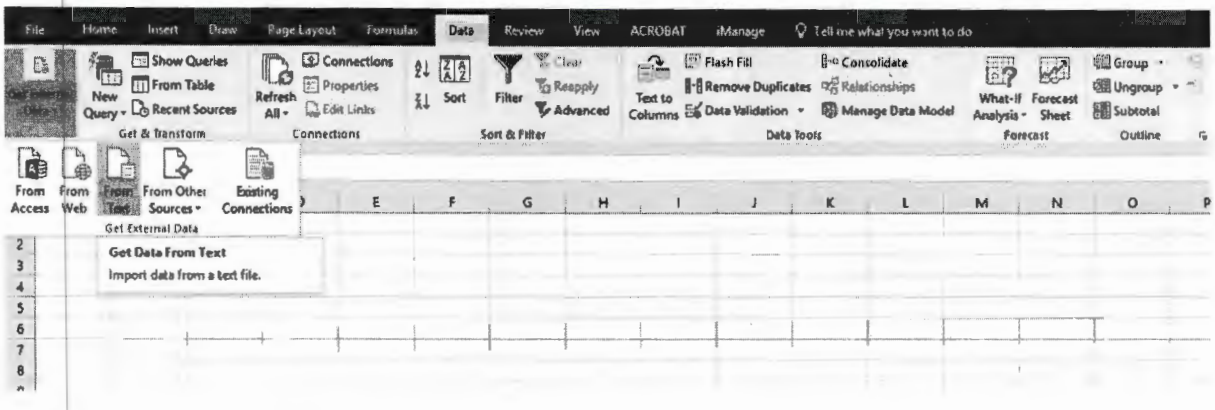
If card security code was purged within 24 hours, does that mean the unauthorized party did not access it?
Not necessarily. The unauthorized party may have accessed payment card security codes if provided to the CRS. However, for a large percentage of reservations, payment card security codes were never provided to the CRS as part of the reservation and would not have been accessible to the unauthorized party. To the extent we were provided with a card security code, the code was purged from the CRS within 24 hours of the creation of the payment record.

Who can I call with follow-up questions?
Should you have any questions, please contact your account manager or call 877-367-2269 toll-free from the U.S. or Canada, or you can call one of our global support numbers available at http://sabrehospitality.com/contact.

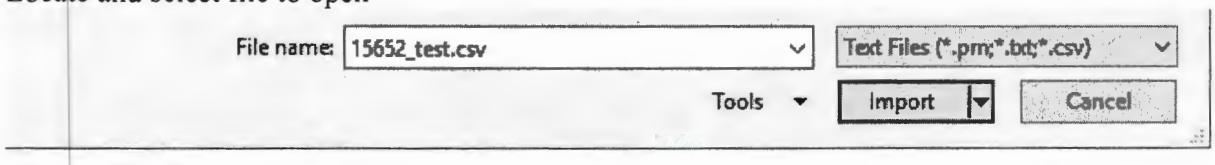
ATTACHMENT F: .CSV Worksheet Instructions for Microsoft Excel

Open Excel and start a new workbook.
To perform import of .csv, use the following steps.
Select Data Tab

Get External Data --> From Text

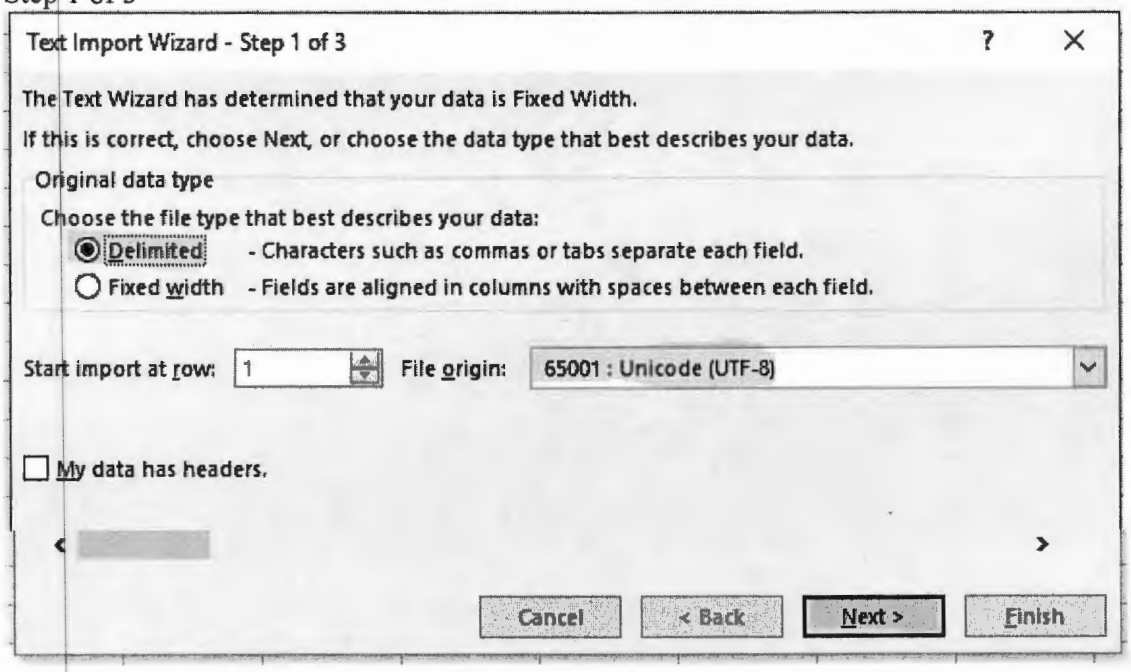


Locate and select file to open

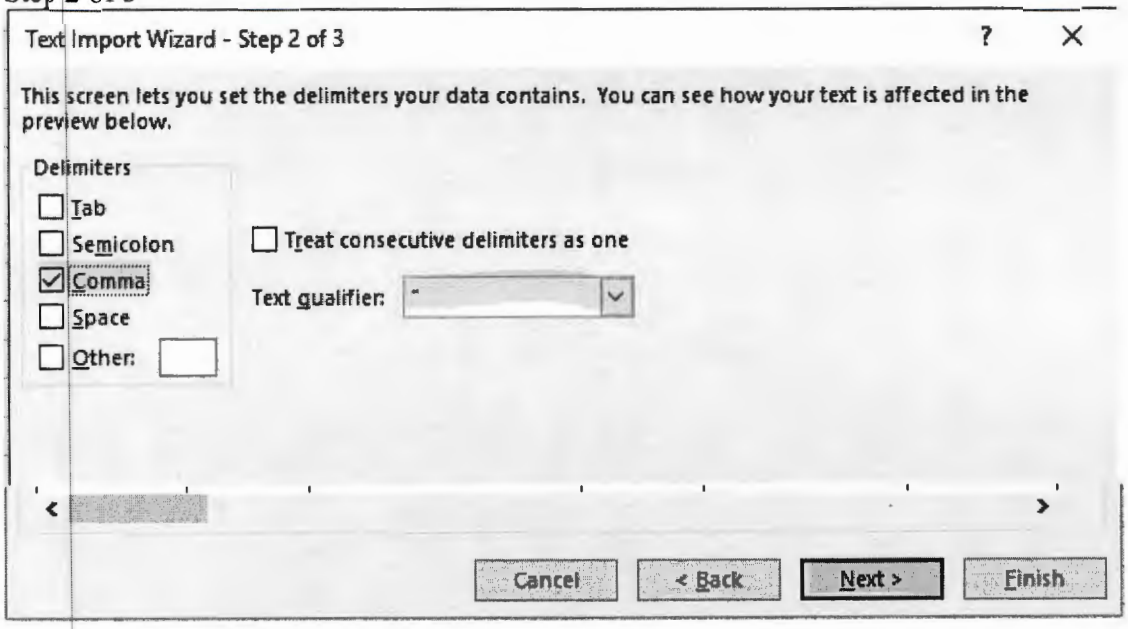


Text Import Wizard dialogue should appear.

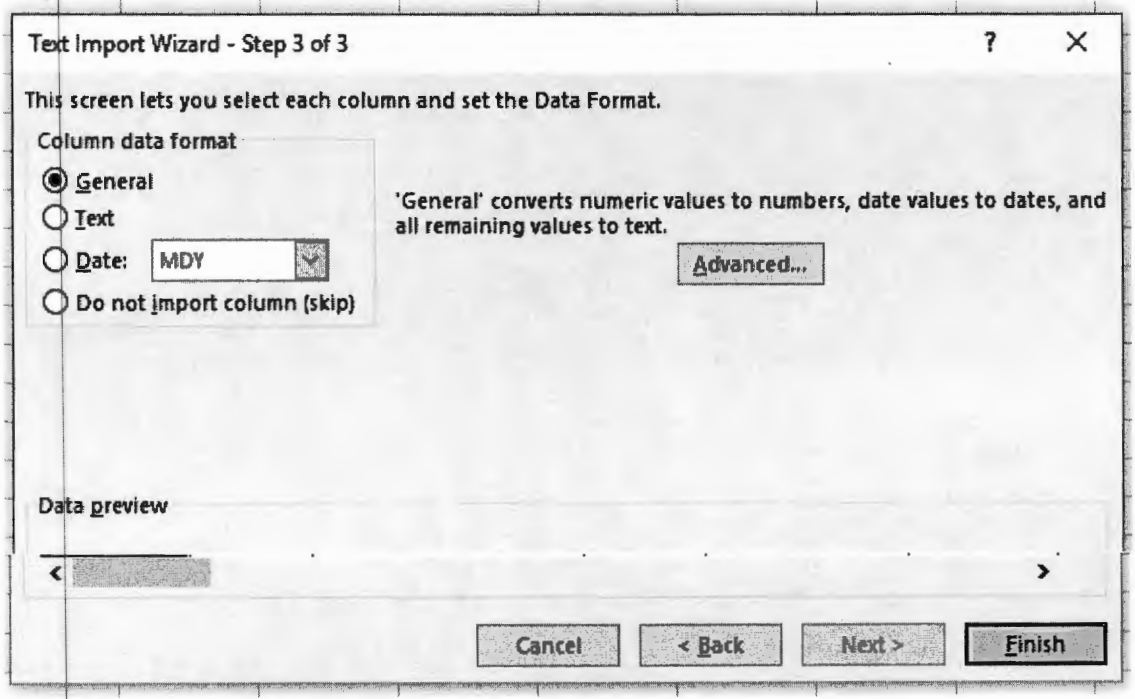
Step 1 of 3



Step 2 of 3



Step 3 of 3


Text Import Wizard - Step 3 of 3
This screen lets you select each column and set the Data Format.
Column data format
General
Text
Date:
MDY
Do not import column (skip)
'General' converts numeric values to numbers, date values to dates, and all remaining values to text.
Advanced...
Data preview
Cancel
< Back
Next >
Finish