FAQs for Release 9.11.2

OVERVIEW

As part of the 9.11.2 release to SynXis Central Reservations (CR), Sabre made changes to the way the SynXis CR manages credit card and payment data for hotels with a CRS/PMS integration. These changes are in keeping with our commitment to periodically review and enhance our security protocols.

With the 9.11.2 release, we have limited credit card access to a single system, either the CRS or the PMS, based on the customers' preferences. **Hoteliers will either access credit card information via the SynXis CR or within their PMS solution. Users are no longer able to access credit card information in both solutions.**

There are three system settings that determine how credit card data is pushed to the PMS from the SynXis CR:

- **Include** = If your hotel is set to "include," then the full credit card data is delivered to the PMS from the CRS after which the credit card data is masked in the CRS. SynXis CR users who have privileged access to view credit card data will only see the last four digits of the credit card number in the Control Center. This setting is recommended for customers who intend to manage credit card information in the PMS, not the CRS.
- **Mask** = If your hotel is set to "mask" then the card data is masked when it is sent from the CRS to the PMS, meaning the PMS only receives the last 4 digits – the rest of the card number is represented by XX's. The full credit card information is still viewable in the CRS. SynXis CR users who have privileged access to view credit card data will be able to view the card details in Control Center. This setting is recommended for customers who intend to manage credit card information in the CRS, but want to view the last four digits of the credit card number in the PMS.
- **Remove** = If your hotel is set to "remove," then the credit card data is not sent to the PMS from the CRS. SynXis CR users that have privileged access to view credit card data will be able to view the credit card details in Control Center. This setting is recommended for customers who intend to manage credit card information in the CRS, not the PMS.

The full credit card number will either be accessible in the PMS or in the CRS. It will not be viewable in both solutions. In addition, Sabre has not changed your setting. Most customers are set to **Include.** To change or review your setting, please contact your account manager or Customer Care.

GENERAL

Q: Why did we make this change?
A: Sabre is committed to a holistic security program and regularly makes updates to enhance the security of the system. With the 9.11.2 release we have limited card access to a single system, either the CRS or the PMS.

Q: How do I know what setting my hotel has? What if I want to change the setting?
A: You can tell based on how the credit card data is handled in the SynXis CR and your PMS. See the descriptions above. If you have questions or would like to change the setting, please contact Customer Care or your account manager.

Q: Does Sabre have a recommendation to switch from Include to Mask, instead of Remove?
A: No. It is up to the hotel based on how they intend to manage credit card data.

Q: What is the default setting (Include, Mask or Remove)?
A: The default setting for a hotel as it is being built, is Include.

Q: How will Sabre handle chain level requests to change attributes across many properties?
A: This is hotel level functionality. If you have a large volume of hotels under a chain that need to be updated, please contact your account manager.

Q: What other resources are available to me?
A: The information regarding these settings are in Help as well.

PAYMENT PROCESSING

Q: What do I do if my PMS does not handle virtual cards?
A: If you need to access virtual cards from an originator such as an OTA, please go to the OTA portal.

Q: If my hotel is set to "Mask," how does that impact tokenization for payment processors to have a current certification with the CRS?
A: If the option is Mask, we will send the PMS something like XXXX-XXXX-XXXX-1234, or all Xs and the last four digits. The PMS cannot read a masked card and cannot therefore tokenize it.

Q: What about PMSs that do not display CVV code?
A: If they don't display a CVV code and you need to access CVV code, then you can configure it to manage card data in the CRS by selecting the settings "Mask" or "Remove."

Q: What if my PMS provider is not PCI compliant?

A: If you have been advised that your PMS partner is not PCI compliant, then you should manage your credit card and payment information in the CRS. Please contact your account manager to update your setting to "Remove" to prevent credit card data from being sent to the PMS.

FAILED INTEGRATION

Q: How can I get credit card information for reservations that fail integration?

A: Review the failure reason in the Interface Health Center. If the reason is a code or mapping issue, please resolve the identified issue and click the reset button in the health center to resend the reservation. If the integration failure reason is not resolved, the reservation is sent via email to the property. In this case, hotels cannot access card data in the CRS.

Q: How do I access the Interface Health Center?

A: It is located by navigating to Manage > Interface Health Center.

Q: Where do I go to figure out why an integration failed?

A: Please review the failure reason in the Interface Health Center.

Q: Who has access to the Interface Health Center?

A: The following roles have access to the Interface Health Center by default: Chain Administrators, Reseller Account Manager and Property Administrator.

LOGIN VALIDATION & AUTHENTICATION

Q: Once the code is delivered to authenticate, how long is it valid?

A: It is valid for 30 days, unless you change browsers or devices, or clear your browser cache. If a user logs in using Internet Explorer during one session and Chrome in another, they would need to authenticate again in Chrome.

Q: Why didn't I receive the security code email when I tried to login?

A: One reason could be that it is in your spam folder. Please see if the email was captured there. Another reason could be an invalid email address. To check the email associated with the account, the user should skip validation step, go to the manage login access link in the upper right hand of the screen (clicking the + next to the user name) and review the email address that is on file with their account. If it needs to be updated, update the account, then log out and log in to request the security code.