¿Qué es el 3D Secure / CES (Comercio Electrónico Seguro)?

Estas siglas corresponden a una iniciativa respaldada por Visa (Verified by VISA) y MasterCard (MasterCard SecureCode) para los pagos por tarjeta de crédito a través de internet.

En un pago a través de internet normal, sin 3D Secure / CES, el pagador solamente ha de introducir datos que figuran en la propia tarjeta (número, caducidad, titular y código CVV/CVC). Y en un pago con 3D Secure / CES, tras introducir los datos que figuran en la propia tarjeta, se redirecciona al pagador a la web del banco con el que tiene la tarjeta, donde ese banco le pedirá una segunda validación de identificación personal. Esta segunda validación es diferente para cada banco (depende de cada banco), y básicamente consiste en un pin, un código por SMS o similar… una información que no está presente en la propia tarjeta, para de esta forma asegurar que el pagador es el titular real de la tarjeta, está realizando efectivamente el pago de forma conocida por él, y que no es un intento de fraude por alguien que hubiera robado la tarjeta.

¿Qué implica?

En los cobros realizados a través del Módulo TPV bajo entorno 3D Secure / CES, no hay riesgo para el comercio (alojamiento) ante una devolución del pagador, sino que es asumido por el banco emisor de la tarjeta, ya que ha sido quien ha verificado la identidad del pagador (no obstante es altamente recomendable recabar un recibo firmado por el pagador en el que figure el importe, el servicio prestado y donde figure nombre y apellidos, dni y firma del pagador que ha de ser el titular de la tarjeta, ya que esta información puede ser requerida por el intermediario de medios de pago).

En los cobros realizados a través del Módulo TPV en entorno sin 3D Secure / CES el riesgo ante una devolución por parte del pagador sería trasladado al comercio (alojamiento), quien en cuyo caso debería demostrar haber identificado al pagador y la tarjeta con la que se ha pagado, como muestra de que dicho pago ha sido realizado conscientemente, de forma aceptada y además se ha disfrutado del servicio (imprescindible en este caso tener un recibo firmado por el pagador en el que figure el importe, el servicio prestado y donde figure nombre y apellidos, dni y firma del pagador que ha de ser el titular de la tarjeta).

¿Porqué no trabajamos siempre en entorno 3D Secure / CES?

El problema viene de que el porcentaje de implantación del protocolo 3D Secure / CES todavía no es del 100%, y tampoco es homogéneo sobre todo para los usuarios Españoles. Esto genera que un porcentaje sensible de viajeros no pueda pagar con el protocolo 3D Secure / CES al no tener su tarjeta habilitada para ello (aclarar que activar el 3D Secure / CES para una tarjeta es gratis siempre, y todos los bancos pueden hacerlo, algunos lo hacen de forma muy rápida incluso son una simple solicitud por teléfono). Además, los pagos sin 3D Secure / CES al ser mucho más rápidos y sencillos tienen una conversión mucho mayor. Es por esto que muchas veces encontramos intentos de pagos que no pueden ser finalizados si se está tratando de cobrar mediante 3D Secure / CES.

También se dan situaciones en las que el comercio (alojamiento) necesita poder realizar un cobro y no tiene delante al pagador para que este pueda aportar ese "código de validación".

Es por esto, que a veces se necesita pasar a entorno NO 3D Secure / CES.

¿Cómo funciona a este respecto AvaiBook?

Por defecto nuestro Módulo de TPV Virtual funciona en entorno 3D Secure, y sólo cuando un comercio (alojamiento) está validado puede solicitarnos el cambio a entorno NO 3D Secure / CES. Y para ello ha de cumplir un protocolo de descargo de responsabilidad, donde se le informa de los riesgos y de cómo actuar para minimizarlos.

¿Y cómo se gestiona el riesgo en los cobros sin 3D Secure / CES?

Existen sectores de alto riesgo respecto del pago sin 3D Secure / CES, ya que un comprador puede adquirir un producto y pagar por tarjeta a través de internet sin entrar en contacto nunca con el vendedor. Como por ejemplo la venta de electrónica, telefonía etc.

Sin embargo, en nuestro sector, el comprador o pagador (viajero) ha de presentarse en el alojamiento para "consumir" el servicio que contrata y paga (su estancia), y por tanto es sencillo verificarlo y anular el riesgo, pidiendo que nos presente la tarjeta con la que realizó el pago y una identificación (tal y como en cualquier comercio en el que pagamos con tarjeta, que nos piden ver la tarjeta y el DNI para verificar que todo es correcto, y firmamos un recibo).

Por tanto, el comercio (alojamiento) con el Módulo TPV en entorno NO CES / 3D Secure ha seguir unas reglas básicas para estar “seguros”:

- Si el pagador está en el alojamiento, ha de verificar la tarjeta e identificación del titular.
- Si el pagador no está presente en el momento del cobro, ha de asegurarse de verificar la tarjeta e identificar al titular en el momento en que llegue al alojamiento
    - Es una buena idea pedir al pagador que envíe un correo electrónico con una foto de la tarjeta + el dni del titular. Es algo sencillo, que hoy en día todo el mundo puede hacer en 2 minutos, y que anticipa cierta seguridad al comercio (alojamiento) de que el pagador (viajero) es el titular real. Esta es una práctica que algunos comercios electrónicos realizan en el control de fraudes.
- Siempre recabar el recibo firmado del cobro (importante que el concepto del cobro refleje el servicio prestado, y que se firme y rellene con nombre y apellidos, y dni), cuando el pagador llegue al alojamiento, y archivarlo durante al menos 12 meses.
- Nunca devolver un cobro realizado por el Módulo TPV por otra vía que no sea el propio módulo.

Trabajando de esta forma, en caso de una eventual solicitud de “charge back”/retroceso de una operación, el comercio (alojamiento) podrá aportar toda la información para enviar al intermediario de pagos y que no haya ningún problema.