

Further background

Canada has a knowledge gap that must be bridged to allow the B2B2C travel distribution network to benefit from EMV 3DS¹ (3DS). By allowing the separation of the Authentication step during the payment process, the major card brands have provided the travel industry with the basic tool set needed to create a safer environment. The knowledge gap is a result of the large number of different steps and suppliers involved to complete a transaction. No one company has a complete overview of the entire process; the 3DS Task Force will address this challenge.

For those who are external to the travel industry, a B2B2C transaction is described as:

1. The cardholder (C) reserves their vacation with their travel agency (B)
2. The travel agency then makes a reservation on behalf of the cardholder with a tour operator (B) who is the actual supplier of the vacation.
3. The tour operator receives the cardholder data only from the travel agency who controls all contact with the cardholder,
4. The tour operator is the actual merchant, so they use the cardholder data received in a card not present (CNP) environment for the authorization and deposit of payment

In the above scenario, it is currently not possible to deploy 3DS as the ultimate credit card merchant has no direct contact with the cardholder. Since travel agencies are responsible for transactions, it is travel agencies who end up covering fraud chargeback costs.

Since change to the workflow is required to deploy 3DS within the B2B2C travel distribution network in Canada, industry consensus needs to be built and this was the reasoning behind the creation of the 3DS Task Force.

Canadian travel agencies right now are literally defenseless, and they are currently losing millions of dollars per year to credit card fraud. Why are travel agencies in such a bad spot? Because almost all their sales are done as what is described as “Card not present” transactions.

The fundamental problem is that travel agencies are almost never the actual merchants in the sale. It is the airline or the tour operator whose products they are selling who is the merchant. Since the actual credit card merchant has no contact with the cardholder, it is currently impossible to apply fraud prevention tools.

Up until now, our Associations have been teaching travel agencies about potential red flags so that they can refuse transactions which might be fraudulent. This results in frequent negative experiences for valid cardholders and less sales for merchants.

Implementation of 3DS will enable travel agents to achieve the same level of protection that other merchants enjoy using the normal chip and pin readers used at all retail outlets. Another benefit of 3DS is that sales volumes will increase through a reduction of the false positives for fraud we are currently facing.

Once consensus is achieved, there will be a major education effort undertaken by our Associations to promote the adoption of the new workflows. Building awareness will be key to speeding up the implementation of 3DS.

It is estimated that this Task Force will speed up the 3DS deployment process by 18 -24 months and will help our industry reduce millions of dollars of fraud losses.

1: Description of EMV 3DS

EMV stands for Europay, Mastercard, Visa. It is a joint effort between Europay, MasterCard and Visa to ensure security and global acceptance so that MasterCard and Visa Cards can continue to be used everywhere.

<https://www.cardinalcommerce.com/3-d-secure-2-0>

3-D Secure is a set of protocols that enables card issuing banks to validate that cardholders are who they say they are, to reduce fraud in Card-Not-Present transactions.

Each card network (Visa, Mastercard, American Express, Discover, and JCB) has their own version of 3-D Secure.



EMVCo: EMV 3-D Secure

<https://www.emvco.com/emv-technologies/3d-secure/>