Circular: NPCI/2018-19/RuPay/030 **09th Jan, 2019**

To All Member Banks – RuPay

Dear Sir/Madam,

Subject: Enablement of RuPay International Global Cards on all DFS enabled E-commerce merchants through second factor authentication (2FA) via "Discover ProtectBuy" solution.

Overview:

In the current scheme of things, International RuPay E-commerce transactions are processed through one factor authentication and this arrangement is available for selected international E-commerce merchants. The liability arising due to one factor authentication is also covered through arrangements with RuPay International card affiliate.

Since the above arrangement is only for selected merchant sites, in order to enable merchant acceptance on all the 3DS enabled international merchants, NPCI has evaluated and implemented enabling second factor authentication (2FA) for all RuPay International card transactions via "Discover ProtectBuy" solution, when transacting on International merchants.

Discover ProtectBuy is based on the 3-D Secure Protocol that enables issuers to verify a Cardholder's identity during checkout through a secure web-based session between the Issuer and Cardholder. The Issuer authenticates the Cardholder's identity in real time.

The attached annexure has the implementations details. This will be implemented w.e.f. 10th Jan, 2019.

All Member Banks are requested to kindly take a note of the same. For any queries, you may please contact Neelesh Gupta at 7506446579 or write at neelesh.gupta@npci.org.in

Yours faithfully,

Vishal Anand Kanvaty
SVP – Innovation & Product

Annexure

Implementation Details:

1. NPCI has done the changes at its PaySecure and Switch end to incorporate two factor authentication in all the international DFS enabled E-commerce transactions.

2. As per this development, 'Card Holder Authentication & Verification value (CAVV)' will be generated by NPCI PaySecure system and sent to DFS. DFS switch will then send this CAVV value to NPCI switch in authorization leg. NPCI switch will validate the CAVV value against the value received.

3. New value "IT" will be introduced in cardholder status tag in Auth_Initiate API call for international transactions, to indicate Bank IAS (Issuer Authentication Server) about the international transactions.

4. In addition to the above, for all international transactions processed through ProtectBuy solution, NPCI would capture CVD2 during authentication process and forwards it to the issuer in Auth_Initiate API call

5. In this proposed solution, ECI indicator value 05 would be passed in Tag 056 of DE-48 for the secure international E-commerce transactions.

   05 – Secure E-commerce transaction with 3D, authentication successful

6. In addition to the above, NPCI systems are also provisioned to facilitate ECI indicator values 06/07, which would be passed to the Issuing Bank only in case of below scenarios.

   Scenario 1:

   06 – Not authenticated security transaction. Merchant attempted to authenticate using 3D secure

   Case A: Merchant has attempted to initiate a ProtectBuy transaction, and for the transactions
   a. Successful Auth_Initiate and Redirection responses received from Issuer IAS system, however
   b. during Auth_Result API call, response status is not received by NPCI PaySecure from the IAS

Auth Initiate Response Status from IAS to NPCI PaySecure	Redirection Status from IAS to NPCI PaySecure	Auth Result Response Status from IAS to NPCI PaySecure	ECI Value	Authentication Scenario
Success	Success	**Not Received**	06	Authentication Attempted

07 – Non-authenticated Security Transaction

Auth Initiate Response Status from IAS to NPCI PaySecure	Redirection Response Status from IAS to NPCI PaySecure	Auth Result Response Status from IAS to NPCI PaySecure	ECI Value	Authentication Scenario
Success	Not Received	NA	07	Unable to Authenticate
Failure	NA	NA	07	Unable to Authenticate
Not Received	NA	NA	07	Unable to Authenticate

Merchant has attempted to initiate a ProtectBuy transaction, and may be, but is not limited to scenarios wherein

a) Card was not eligible for ProtectBuy Authentication. This may be due to one of the following reasons:
   a. the cardholder is not enrolled in ProtectBuy,
   b. the card number is not valid, or
   c. the IIN is not set up for attempts processing.
b) Issuer's IAS not able to complete the authentication request due to any of the reasons such as
   a. the authentication request was routed to the wrong IAS,
   b. IAS was not able to establish a TLS session with cardholder browser
   c. a system failure occurred that prevented proper processing of the authentication request.
c) Authentication failed due to
   a. Cardholder fails to correctly enter the authentication information within the Issuer-defined number of entries,
   b. the cardholder cancels the authentication page or a failed authentication may indicate a fraudulent attempt and the merchant should not submit the transaction for authorization.

7. As presently, only successful authenticated ECI value (05), is sent to Issuer switch, NPCI switch will only forward the ECI value 05 to the issuer Banks for necessary approvals.

8. If the Issuing Bank desires to validate the transaction basis ECI indicators 06/07 at authorization level, the Banks will have to follow below prerequisites:
   a. Member Bank will need necessary development at their switch.
   b. The Bank will have to undergo separate certification with NPCI.
   c. The liability shift for the Protect Buy transactions will be assigned to the Issuing Bank in case of fraudulent transactions

d. Issuing member needs to refer to International Operating Manual for Dispute & transaction Liability Guidelines.

9. Non-secure E-commerce transactions would be declined at NPCI switch end. NPCI switch will be provisioned to facilitate ECI indicator value 08 for all such transactions

10. None of the international e-commerce transaction would be processed through One Factor Authentication post implementation of ProtectBuy solution.

11. From Issuing Bank perspective, for international E-commerce transactions, hashing mechanism would remain the same as it is currently implemented for domestic transactions and there will not be any separate change involved for implementing hashing for ProtectBuy solution.

12. Hash code generation and validation would be done at NPCI end from Acquirer perspective for all the international transactions post implementation of ProtectBuy.

13. All the above mentioned changes would be applicable for the Banks issuing international RuPay cards.

14. As the developments are done at NPCI internal systems, there will not be any change from Bank IAS and switch perspective for implementing ProtectBuy solution.

15. Since ProtectBuy would enable second factor authentication (2FA) for all the international transactions performed on DFS enabled merchants, all these transactions would be authenticated through OTP.

16. Since these transactions could be done across borders, in order to send the OTP to the consumers located within and outside India, it is recommended that Issuer IAS system builds the mechanism to send OTP to the registered email id as well as mobile number of the customer. Also to enable use of international RuPay cards.