Regulatory Hotline

August 27, 2014

ONLINE CREDIT CARD SECURITY: CLARIFICATORY DIRECTIVE FOR E-PAYMENTS

- Online Credit Card Payments - RBI clarifies the requirement for use of 2nd level authentication by merchants / vendors.
- 2nd level authentication required where the underlying transaction is domestic – i.e. between two Indian residents.
- Transactions using an Indian issued card, and between Indian residents to be settled in Indian currency by an Indian acquiring bank.

On August 22, 2014, the Reserve Bank of India ("**RBI**") issued a directive[1] ("**RBI Directive**") clarifying the requirements for additional authentication / validation for credit card transactions. In response to the questions raised by the Association of Radio Taxis in a letter to the RBI earlier this month, the RBI Directive specifies that the RBI mandated additional authentication / validation requirements will apply, in every card not present ("**CNP**") transaction, where an Indian credit card is used to pay for a transaction that is essentially between two Indians.

Credit cards, with their origin in the early 1900s, have been in use in India since the 1980s and have seen an immense growth in the number of users, as well as merchants accepting credit card payments over the past few years. The growth of online services and marketplaces has provided further impetus to the use of credit cards for everyday transactions.

CNPS AND ADDITIONAL AUTHENTICATION / VALIDATION

With both E-Commerce and telemarketing growing rapidly in India, an increasing number of businesses, whether service or product based, require payment online or via phone – leading to CNP transactions.

A CNP transaction is essentially one where the merchant does not have access to the card being used because the customer and the merchant / service provider are not physically in the same location, making it difficult for the merchant / service provider to verify the identity of the customer. There could be situations in which payments and transactions are completed without the knowledge or authorization of the actual holder of a credit card. A CNP transaction would include transactions online, over the phone, over mail etc.

Taking heed of the growing number of incidents of credit card fraud, especially via online payment portals, the RBI issued a notification in February 2009[2], mandating the use of an additional authentication / validation system (also referred to as 2nd level authentication / 3D verification) for online CNP transactions. The additional authentication / validation was to be obtained using information that was not visible on the credit card itself, i.e. information known or available to the holder of the card but not printed on the card. One time passwords, internet banking passwords are examples of 2nd level authentication. Further, banks were also required to put in place an online alert system which would notify the cardholder of any CNP transaction for INR 5000 or above. The requirement for this system of additional authentication, was also extended to interactive voice response (IVR) transactions, typically carried out over telephones, and the requirement for online alerts has been extended to all CNP transactions.

APPLICABILITY OF REQUIREMENT FOR 2ND LEVEL AUTHENTICATION

In October 2010[3], the RBI issued a clarification which provided that the requirement for additional authentication would apply to all transactions where:

(a) The card was issued in India; **and**

(b) There was no outflow of foreign exchange contemplated.

Therefore, where both of the above requirements were met, additional authentication / validation became mandatory – irrespective of whether the payment gateway / website which processed the transaction was domestic or international. However, the requirement did not apply where:

- the cards in use were issued outside India, even if such cards were used on Indian websites.
- the cards issued in India were used to buy goods / services outside India.

Online merchants have not been too happy with the 2nd level authentication requirement for several reasons, important of which were:

- Obtaining a second level authentication requires more time and effort for a customer as opposed to a simple click through transaction

Research Papers

The Tour d'Horizon of Data Law Implications of Digital Twins
May 29, 2025

Global Capability Centers
May 27, 2025

Fintech
May 05, 2025

Research Articles

2025 Watchlist: Life Sciences Sector India
April 04, 2025

Re-Evaluating Press Note 3 Of 2020: Should India's Land Borders Still Define Foreign Investment Boundaries?
February 04, 2025

INDIA 2025: The Emerging Powerhouse for Private Equity and M&A Deals
January 15, 2025

Audio

CCI's Deal Value Test
February 22, 2025

Securities Market Regulator's Continued Quest Against "Unfiltered" Financial Advice
December 18, 2024

Digital Lending - Part 1 - What's New with NBFC P2Ps
November 19, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

Vyapak Desai speaking on the danger of deepfakes | Legally Speaking with Tarun Nangia | NewsX
April 01, 2025

- An increase in the rate of transaction failures, as the customer's bank may not always be able to process the authentication.

Also, 2nd level authentication particularly affected merchants who needed to receive periodic payments from customers, such as a monthly subscription charge. Sans the 2nd level authentication, the customer's credit card would be debited automatically. With the introduction of this authentication requirement, the customer was required to enter the one-time password or any other login / password combination for each transaction, which made it easier for a customer to cancel the subscription if she/he chose not to continue subscription. In this respect, the introduction of the 2nd level authentication was a welcome measure considering the number of consumer complaints against merchants/websites that refuse to cancel subscriptions despite the consumer explicitly asking them to do so.

MARKET PRACTICE BY SERVICE PROVIDERS

It appears that some players in the industry – both merchants and service providers, may have structured their businesses by receiving payments in an offshore entity. Since the authentication requirements do not apply to transactions with entities outside India, additional authentication / validation would not be required. In such cases, while the prices may be displayed in INR at the time of purchase of the product / services by the customer, the amount is paid in foreign currency. Some of these structures may have been validly structured by relocating operations outside India, while some may have been structured only by arrangement with the payment gateway operators.

Recent news reports also suggest that one industry segment that was particularly affected by such practices was that of radio taxis. Domestic radio taxi service providers in India, like any other domestic service providers, were required to ensure that the additional authentication requirements were met for CNP payments. However, an international company having tie up with taxi drivers in India and operating an online app for bookings, appears to have structured its operations in a manner where the 2nd level authentication was not required even for payments to be made to the taxi drivers.

An association of radio taxis has brought such practices to the attention of the RBI recently, and the said RBI Directive seems to be a reaction to this complaint.[4]

RBI DIRECTIVE

The RBI Directive issued last week re-iterates its previous clarification on international payments, and states that despite the same, many companies appear to be effecting CNP transactions without additional authentication / validation measures, by following business / payment models which are resulting in foreign exchange outflow, even where the underlying transaction itself:

- consists of *a card that is issued in India;*
- *is used for the purchase of goods and services offered by a merchant / service provider in India*.

Addressing such transactions, the RBI Directive states that:

"*Such camouflaging and flouting of extant instructions on card security, which has been made possible by merchant transactions (for underlying sale of goods / services within India) being acquired by banks located overseas resulting in an outflow of foreign exchange in the settlement of these transactions, is not acceptable as this is in violation of the directives issued under the Payment and Settlement Systems Act 2007 besides the requirements under the Foreign Exchange Management Act, 1999*"

The RBI Directive further provided that where cards issued by banks in India are used for making CNP payments towards purchase of goods and services provided within the country, such transactions should be settled in Indian currency and the acquisition of such transactions should also be through a bank in India.

Merchants have been given time until October 31, 2014 to comply with the instructions of the RBI.

CONCLUSION – UNANSWERED QUESTIONS

Though the RBI Directive has clarified that 2nd level authentication is mandatory for transactions undertaken for an Indian issued card used towards the purchase of goods and services provided within the country, a number of models commonly adopted by E-Commerce businesses may not always satisfy such a requirement. For example there are a number of global platforms based on a market place model, that aggregate content, services and even products for an international market and make them available to the customers for download or sale.

If an Indian resident offers certain content, say a mobile application on a platform based outside India, and another Indian resident purchases the software application, through the platform via an international payment gateway – would the transaction be considered as one between two residents that falls within the ambit of the RBI Directive? Or would it be considered a transaction between an Indian resident and the foreign platform – which does not fall within the ambit of the RBI Directive? It remains to be seen how the RBI will address such questions. Further, in the coming months it will also be interesting to observe whether the RBI considers easing the process of conducting online / CNP transactions, perhaps waiving the 2nd level authentication for transactions involving smaller amounts.

– E-Payment Practice Group

You can direct your queries or comments to the authors

[1] DPSS.PD.CO. No.371/02.14.003/2014-2015
[2] RBI / DPSS No. 1501 / 02.14.003 / 2008-2009
[3] RBI / DPSS No.914 / 02.14.003 / 2010-2011
[4] http://auto.economictimes.indiatimes.com/news/aftermarket/radio-cabs-allege-fema-violation-by-uber/39921543

Vaibhav Parikh, Partner, Nishith Desai Associate on Tech, M&A, and Ease of Doing Business
March 19, 2025

SIAC 2025 Rules: Key changes & Implications
February 18, 2025

DISCLAIMER

The contents of this hotline should not be construed as legal opinion. View detailed disclaimer.

This Hotline provides general information existing at the time of preparation. The Hotline is intended as a news update and Nishith Desai Associates neither assumes nor accepts any responsibility for any loss arising to any person acting or refraining from acting as a result of any material contained in this Hotline. It is recommended that professional advice be taken based on the specific facts and circumstances. This Hotline does not substitute the need to refer to the original pronouncements.

This is not a Spam mail. You have received this mail because you have either requested for it or someone must have suggested your name. Since India has no anti-spamming law, we refer to the US directive, which states that a mail cannot be considered Spam if it contains the sender's contact information, which this mail does. In case this mail doesn't concern you, please unsubscribe from mailing list.