Press release

# Risks involved in making online payments and how to secure it

*Source: Deccan Chronicle*

**Find the link of the news below:**

https://www.deccanchronicle.com/business/companies/200818/risks-involved-in-making-online-payments-and-how-to-secure-it.html

Mumbai, August 20, 2018

Creating new technical challenges for businesses, payment processors, and customers - and security is a critical area of focus.

Creating new technical challenges for businesses, payment processors, and customers - and security is a critical area of focus.

**Security challenges in the online payments space and overcoming them with smart solutions**

Online payments have made buying and selling simpler and more efficient for merchants and consumers, and the contribution of digital commerce to the global economy increases with each passing day. Moreover, with smartphones, peer-to-peer payments have become more convenient as mobile payment solutions and e-wallets continue to fuel the demand for quick multi-currency and cross-border payment solutions. This intensifying demand, and the scale of online transactions in both the B2B and B2C space, is creating new technical challenges for businesses, payment processors, and customers - and security is a critical area of focus.

**Fraud and data theft mitigation: security measures to make online transactions safer**

The Indian e-commerce has been growing in leaps and bounds. As per the recent economic survey by the Indian government, the sector grew at 19.1% during 2016-17 to touch USD 33 Billion. With the growth of e-commerce, online or 'cardless' transaction methods have become widely popular among consumers due to the level of ease and speed with which they allow them to make payments – and the growth of

the sector has also enabled businesses to reach new buying audiences, online, across social media and internationally.

The flipside of this growth, however, is that businesses need to be continuously aware of the risk that fraudulent activities present. Fraud not only impacts consumer confidence and trust, but also has a direct impact on businesses' revenue. As per the survey by CyberSource, businesses in North America stand a threat of losing up to 0.8 per cent of their total revenue due to frauds, while in India the threat looms between 4 per cent and 5 per cent.

Payment gateways, which provide the technology that processes online payments, have a fundamental role to play in keeping online businesses and their customers safe from fraudulent activity. Payment gateways use antifraud software and algorithms to identify potentially fraudulent transactions, and prevent these transactions from taking place. In this highly complex space, however, not all antifraud protections are equally powerful. The strongest antifraud mechanisms tend to have a number of characteristics:

They're proprietary – built and maintained in-house by the payment gateway – which brings speed and agility in being able to adapt and adjust the software in response to the ever-changing nature of security threats.

They overlay data from card networks, banks and businesses themselves onto their own software, providing a richer, more nuanced degree of protection.

They integrate with other existing consumer protections, such as 3DSecure, so that the consumer is able to remain protected from all angles.

Recognising that businesses are likely to have a detailed understanding of their customers and their behaviour, they offer controls to the merchant that allow them to add further layers of personalised protection, and ideally also to place transactions on hold (rather than declining them outright) so that the merchant is able to investigate potentially problematic transactions.

These features work to keep the customers' payment data safe, and protect online businesses from chargebacks: chargebacks arise when a consumer sees fraudulent activity on their card, and claims the money back from their bank. The online business may have already shipped the product to the fraudster, and may also be liable for the chargeback – and so this scenario is clearly one that does damage to the business, financially and reputationally.

Another aspect that's often over-looked – but is nonetheless absolutely critical – is that payment gateways should not only prevent the fraudulent transactions from taking place, but should also minimise the number of legitimate transactions that are also declined by the antifraud controls.

Declines of this nature – where the transaction itself is genuine, but was declined by the payment gateway's antifraud protection – directly impact the business' revenue. The genuine transaction is lost, and along with it the customer's confidence in and loyalty towards the business also takes a hit. For this reason, it's essential that businesses choose a payment gateway that has a high transaction success ratio – or

face losing both revenue and customers. After all, safe customers keep businesses secure.

Consumer data security is a top priority for businesses and governments around the world, and emerging technologies like blockchain are well-positioned to support the global digital economy and financial ecosystem in this respect.

**Blockchain can bring a halt to frauds and data breaches**

Having already begun to deliver its promise of disruption in the banking and financial services domain, blockchain technology is also being leveraged for strengthening online payments infrastructure and keeping customer data safe. Blockchain provides a digital, decentralized ledger that records each and every transaction using cryptography.

Thus, with no single central entity controlling these information blocks, they are invulnerable to security leaks and tampering. For example, consumers' digital identities are secured and cannot be stolen or tampered with, and the transparency and visibility inherent in blockchain means that past fraudulent behaviours can be identified and that information used to prevent the same actor from being able to undertake further fraud.

Overlay machine-learning onto this foundation, and there is the potential to bring even greater accuracy to protecting businesses and consumers against fraudulent behaviour.

Different technologies continue to come together to build a robust and secure online payments ecosystem globally. An amalgamation of the right solutions matched to specific situations can drive quicker, smarter, secure, and more efficient payment processing; thereby boosting consumer confidence and their reliance on digital payments.

This in itself drives innovation, with intelligent technological tools like blockchain and artificial intelligence expected to play central roles in the evolution of the payments infrastructures that we are all becoming so reliant on.

**About Lyra:**

Founded in 2001 by Alain Lacour, Lyra secures e-commerce and proximity payments and develops value-added services to manage transactions and POS equipment on a daily basis. Based in Toulouse, Lyra is present internationally with 10 subsidiaries (Algeria, Germany, Brazil, Chile, Spain, India, Mexico, Argentina, Colombia and Peru). The group has over 250 employees for a turnover of €53M in 2017.
Lyra's key figures:
Over 10 billion payments secured and transmitted in 2017 worldwide
Over 50,000 e-merchants
Over 3,000,000 payment terminals worldwide
Lyra's services are certified PCI DSS, Visa Merchant Agent and approved by GIE Cartes Bancaires.
http://www.lyra.com