Team SPOT got the opportunity to speak with Colonel Inderjeet Singh, an established Thought Leader in the industry and a distinguished speaker in various national and international forums. An information security expert with over 26 years of experience, Colonel Inderjeet Singh used to work in military intelligence with the Ministry of Defence before moving to corporate. He shared with us some insights into payment security and fraud in the Indian market and how to overcome them.

Interview: Fighting Payment Frauds - Fresh Insight

Q1. What are some of the key concerns on payment security and fraud in the Indian market at the moment?

A1. Inderjeet Singh: *In my opinion some of the key concerns on Payment Security and Fraud are:*

1. Cyber-security is one of the most critical challenges faced by stakeholders of the digital payment ecosystem. With more and more users preferring digital payments, the chances of getting exposed to cyber-security risks like online fraud, information theft, and malware or virus attacks are also increasing. Lack of awareness and poor digital payment ecosystem are some of the primary reasons that have led to increase in these attacks.

2. Back-end lack of technology adoption and implementation by banks, who are still struggling with data Analytics, AI and Machine Learning

3. Lack of Cyber threat intelligence

4. Existing rules are woefully inadequate in their scope and application to effectively deal with potential privacy concerns posed by digital payments applications and services.

Q2. How can those concerns be mitigated?

A2. Inderjeet Singh: *Some of the suggested steps which could be taken to overcome challenges of payment security and fraud are:*

1. There is an urgent requirement of robust regulatory framework to ensure payment security and fraud management

2. Effective customer grievance redressal framework

3. Implementation of foolproof security measures to instill confidence and trust amongst customers making online payments

4. Customer education and awareness. Banking System should instill incentives for large participation and benefits similar to cash transactions, such as ease of use, universal acceptability, perceived low cost of transaction, convenience and immediate settlement, are some measures that can help ensure long-term success for digital payments.

Q3. In your opinion, what are some of the key kinds of payment fraud which are prevalent in the Indian market currently?

A3. Inderjeet Singh: *Cyberattacks have grown significantly in sophistication and persistence (on average, attacks stay undetected for about 200 days). Some of the prevalent payment frauds are:*

1. Identity Theft – Persons (either in companies or privately) who are not entitled to know the bank details of another person or the company get access and use them in fraudulent ways. This could be children using the online banking or credit card details of their parents for shopping online or employees using corporate bank accounts for gambling.

2. Phishing – Growing number of professionals are focused on obtaining the secret online banking details of bank consumers such as their user names and passwords on one hand but also their security confirmation codes such as TANs. These types of fraud patterns are usually driven by malware on the victims' cell phone or computer but also by "clever" phone calls to victims (so called "social engineering"). This *type of fraud is highly developed and organised these days.*

3. Account Theft – Man-in-the-middle attacks are even more sophisticated. These involve hackers muscling in on communications between customers and merchants.

4. Clean fraud – Clean fraud's name is misleading, because there's nothing clean about it. The basic principle of clean fraud is that a stolen credit card is used to make a purchase, but the transaction is then manipulated in such a way that fraud detection functions are circumvented.

5. Affiliate fraud – There are two variations of affiliate fraud, both of which have the same aim: to glean more money from an affiliate program by manipulating traffic or signup statistics. This can be done either using a fully automated process or by getting real people to log into merchants' sites using fake accounts. This type of fraud is payment-method-neutral, but extremely widely distributed.

6. Triangulation fraud – During triangulation fraud, the fraud is carried out via three points. The first is a fake online storefront, which offers high-demand goods at extremely low prices. The second corner of the fraud triangle involves using other stolen credit card data and the name collected to order goods at a real store and ship them to the original customer. The third point in the fraud triangle involves using the stolen credit card data to make additional purchases.

7. Merchant fraud – Merchant fraud is another method which must be mentioned. It is very simple: goods are offered at cheap prices, but are never shipped. The payments are, of course, kept. This method of fraud also exists in wholesale. It is not specific to any payment method, but this is, of course, where no-charge back payment methods (most of the push payment types) come into their own.

Q4. In your opinion what are some of the key methods available for mitigating payment fraud?

A4. Inderjeet Singh: *Some of the methods available for mitigating payment fraud are:*

1. Machine learning with big data analytics

2. Deep learning form fraud detection will reduce frauds by substantial number

3. Blockchain technology once implemented would be a major game changer for reducing payment frauds.

4. Use of AI would be the next step

Q5 What are your expectations from participation at the upcoming SPOT Forum (taking place on 29th Nov 2017 at Sofitel BKC in Mumbai)?

A5. Inderjeet Singh: *Topic chosen is really fantastic and would be able to generate a lot of interesting discussion – especially with banking sector and cyber security experts on the same platform.* ■

Webpage link
http://spotforum.in/2017/09/11/fighting-payment-fraud-fresh-insight/

Colonel Inderjeet Singh is the Chief Cyber Security Officer and Head of the Cyber Security Center of Excellence at Vara Technology. In this role he is instrumental in building the Cyber Security Business Unit for the Group. He is working on the disruptive technologies in the Cyber Security Space for securing IT networks, Smart cities and Critical Information Infrastructure.

He served in the Indian Defence Forces, is Alumnus of IIT Kharagpur and Symbiosis Institute of Management. He is an experienced Information Systems professional with experience of more than 27+ year across wide spectrum of areas spanning Information Security ,Risk Management, Cyber Security, Cyber Forensics, Cyber Warfare, Cyber Terrorism, Expertise in SOC and CERT, Internet of Things (IoT) including IoT Security, Blockchain and Cryptonomics, Machine Learning and Artificial Intelligence and Smart Cities.

He has held prestigious appointments while in Indian Army and has been CIO of E-Commerce Company. He has also served in United Nation Mission in Democratic Republic of Congo.

He is visionary for Start-Up Incubation, Entrepreneurship Development, Strategic Consulting and New Technology Evaluation for commercial viability. He is a Subject Matter Expert on latest innovative Technological domains and effectively managed mission critical projects

He has consistently delivered mission-critical results in the field of in Information Security Management, Cyber Security, Cyber Warfare and Cyber Risk Management.

He is a Council Member of CET (I) and fellow of IETE, IE, Member CSI and Executive Council Member Society for Data Science, Founder of Cyber Watch India, Member ISACA, IEE, ISOC, IoT4SCTF, CCICI, IETF, USI and many other professional bodies.

He has been consistently been awarded while in Army and was awarded "Magnificent CIO of the Year "Award in year 2016.