Emerging Trends in Cyber Frauds in India

Case Studies from Mumbai

By

Nandkumar Saravade, IPS,
West Bengal Police Directorate, Kolkata

Dr. Pradnya Saravade, IPS,
Deputy Commissioner of Police,
Enforcement, Mumbai

1. Introduction

1.1 Information Technology has become the new *mantra* of modern India. The groundswell of interest in this new knowledge tool, which is seen to hold the potential for solving India's age-old problems of poverty and lack of education, can be discerned by even a casual observer of the Indian society. Indian industry, businesses, financial organizations and even the ordinary citizens have been embracing Information Technology rapidly and without reservation. With this techno-trend, come new problems of law enforcement for the police organizations in the country. There is a bewildering variety of criminal behaviour in the cyberspace, which seems unhindered by national boundaries. This article is an attempt to report and analyse the trends in cybercrime, as have come to notice in Mumbai Police Cybercrime Cell.

1.2 The current PC penetration in India is around 5.8 per 1000 persons and rapidly improving. The PC availability for the average user goes up if one considers usage through Internet cafes. NASSCOM projects a figure of 50 million Internet users at the end of 2004. An IMRB study estimates the total number of cybercafes in the top 16 Indian cities to be around 12,000. Even with our nascent computer usage in areas like retail trade and other e-commerce applications, we are already seeing an emerging trend in the frauds being perpetrated.

1.3 The Internet, as a medium, has its inherent attractions for fraudsters - it is perceived to be faceless and the involved transactions can be of large value. Frauds can be committed swiftly, making it that much more difficult for law enforcers to get to the fraudster. The speed of transactions on the Net enables the Net criminals to easily change their locations across political boundaries after committing crimes. Crimes on the Net, therefore, need radically different enforcement solutions for tackling and containing them. Speedy international co-operation for quick intervention, speedy trials to bring the criminals to book and capable and effective law enforcement teams to understand and intercept Net crimes, are therefore, the needs of the near future.

1.4 As a rapidly growing economy which is showing great potential for improving the living standards of its people, India must guard against emerging Net frauds, in order to nurture the good sentiments generated around its economic growth. Since criminals on the Net respect no geographical boundaries, even national security becomes our concern. Now, we shall see the implications in two such representative cases recently registered with the Mumbai Police Cyber Crime Investigation Cell (CCIC).

2. Case Studies

a) Case Study No.1

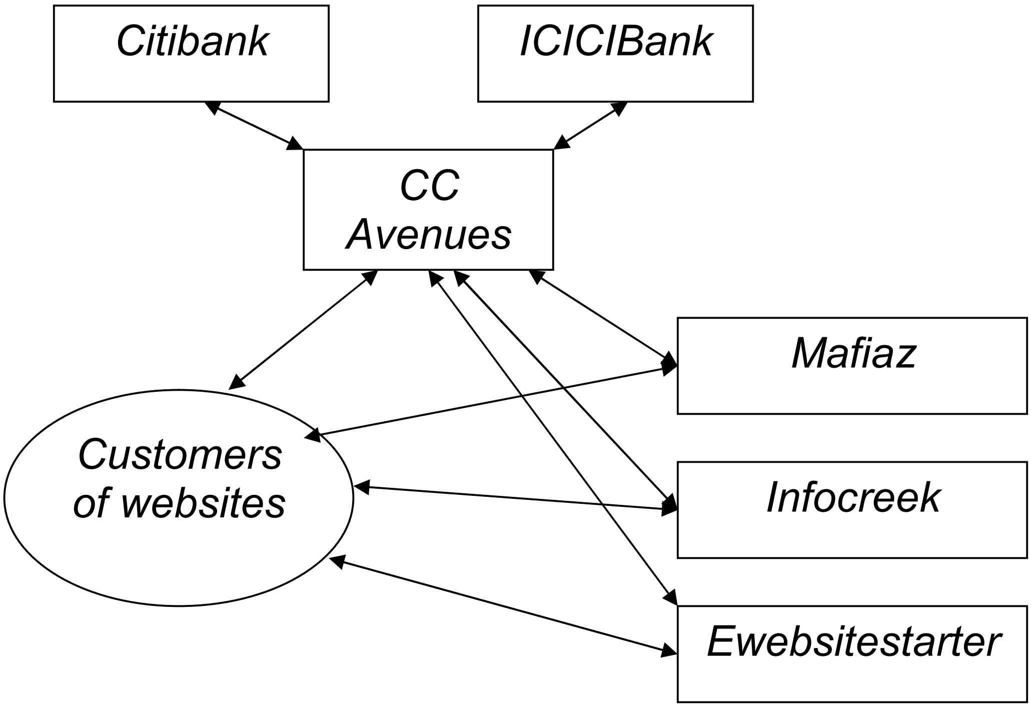
2.1 CC Avenues (CCA), a Mumbai-based company, runs what is known as a 'Payment Gateway' on their website, for providing online credit card authentication services to merchants who accept online credit card payments. It leads the customer to the site of either of two Banks, viz. Citibank and ICICIBank, which run such a facility in India. It functions like a middleman getting online transacting customers for the Banks. It has a responsibility of verifying the genuineness of such customers before they are allowed to use the payment gateways.

2.2 In May 2002, one young engineering student, AT, executed an agreement with CCA for facilitation of online payments to him for graphic designing services offered by him through his website *Mafiaz*. He then proceeded to create fictitious customers to his own website under different names, with stolen or algorithm-generated credit card numbers, and received payment of Rs. 3,11,508 from CCA, between November

2002 to February 2003. CCA received chargebacks (credit card equivalent of a bounced cheque) after two months, for all the credit cards used on *Mafiaz*. By now, AT is no longer available at his address stated in the Agreement.

2.3 AT floated two more outfits, titled *Infocreek* and *eWebsitestarter*, which collected from CCA Rs.9,53,651 in an account in Pune and Rs. 4,22,978 in another account in Hyderabad, respectively. *Infocreek* was active from March 2003 to May 2003, whereas *eWebsitestarter* functioned for two months from May 2003 onwards. Around middle of January 2003, AT floated *Domaindealz*, another of the now-predictable web designing firms. He operated his technique to collect credit of Rs. 1,41,342 in his Bank Account at Hyderabad, for his fictitious customers. It was in relation to transactions in this account, i.e. *Domaindealz*, that CCA finally became suspicious. After receiving some chargebacks in this Account, CCA conveyed their suspicions to the police.

2.4 A trap was laid and AT was lured to the CCA's office for receiving an outstanding cheque of Rs. 40,000. The hunter became the hunted and was nabbed. During interrogation by the police, he confessed to having posed as owner/proprietor of the aforesaid firms and having collected the entire defrauded amount from his various Bank Accounts. The flow diagram of the transactions is depicted below.



b) Case Study No.2

2.5 Indian Railway Catering and Tourism Corporation (IRCTC) has recently launched a Net facility for booking railway tickets wherein a customer registers himself at the IRCTC's website (http://www.irctc.co.in/), giving, among other details, his permanent postal address and his e-mail address. He can then proceed to book tickets online, which are delivered by a courier company to the registered address. This mode of booking tickets offers unmatched convenience, in return of a nominal charge, one can see for oneself the availability of trains on a route, their timings, accommodation availability and the fare chargeable and can also specify the berth to be booked. The popularity of this service can be gauged from the fact though started as late as August 2002, the corporation has clocked 4.8 lakh registered customers and was transacting business worth Rs 45 lakh every day, through the sale of an average figure of 3300 tickets. It has emerged as the leading e-commerce entity in India. It has plans to offer sale of tickets through mobile phones. IRCTC uses the payment gateway facility of two Banks for their online customers.

2.6 A case was reported to the Mumbai Police Cyber Crime Investigation Cell by IRCTC on 11 September 2003. One 'R' had purchased tickets worth Rs.25,000 for Ajmer and back through the IRCTC online Booking facility, using a credit card. IRCTC had delivered the tickets to a shop in Heera Panna Shopping Centre at Haji Ali in Mumbai and the tickets were utilized. Similarly, some different identities, 'N', 'L' and 'T' had also booked railway tickets in II and I AC coaches to various destinations and taken delivery of the tickets and used them.

2.7 IRCTC received chargebacks, declining payment, on all the credit cards used by these customers. The chargebacks are normally received only a month after the transactions. The real owners of the credit cards had asserted that they had never purchased the tickets. Someone had apparently used the credit card numbers to purchase tickets at the IRCTC site. IRCTC, being the online merchant, had to bear the losses in all the above cases.

2.8 During investigation, it was possible to locate the actual person who had booked the tickets through the normal investigative techniques, link him to the crime through the acknowledgement slips signed by him and the record of his logging on to the IRCTC site, from his office computer, which he had used to connect to the internet.

c) <u>Learning experiences in case no. 1</u>

2.9 In the first case study, some serious flaws were found in the way payment gateway banks were ensuring authenticity of credit card transactions. The usual route for such verification is by getting authentication from the card issuing Bank on three parameters - the Card's Number, Card Expiry Date and the CVV2 Number. A brief discussion on the CVV2 number is in order here.

2.10 Credit Verification Value (CVV2)/ Credit Verification Code (CVC2) authentication involves the MasterCard/Visa credit and debit cards, which carry a 3-digit non-embossed number on the back of the card. American Express cards carry a 4-digit number on the front of the card. This number is not included in the data contained on the magnetic stripe of the card and is not printed on credit card statements or anywhere else. The merchant asks the customer for the CVV2 code and then sends it to the card Issuer as part of the authorization request. The card Issuer checks the CVV2 code to determine its validity and then sends a CVV2 result back to the merchant along with the authorization.

2.11 It was found that, in the instant case, one of the payment gateway banks was authenticating the online transaction even on invalid CVV2 Numbers, indicating that actually no CVV2 check was being done. On the other hand, the other payment gateway was not even requiring the customer to enter the CVV2 number before authenticating the card /transaction.

2.12 Credit Card companies classify transactions as 'Card Present' and 'Card Not Present'. The categories are self-explanatory. In the second category, presence of a physical credit card is not necessary and only the card number is sufficient to close a deal. All credit card transactions on the internet are of the latter category and are rising rapidly. These transactions are inherently less secure. The checks done during the verification of cards used online, have, therefore, to be more stringent than those done while concluding physical transactions.

2.13 It was found during investigation that Mastercard and Visa card companies have not made it mandatory for all the Card Issuing Banks to verify the CVV2 number before approving the online transactions. It is common knowledge that card numbers and their expiry dates are freely available on the Chat Rooms on the Net. Card numbers can also be easily generated using known algorithms. On the other hand, CVV2 numbers cannot be generated through algorithms and neither are these available easily.

2.14 A glaring flaw that was found during the investigation of this case was the casualness with which CCA made agreements with online merchants. There was no verification by CCA of persons, addresses or even the supposed services/merchandise being offered online. Investigation revealed that no valid services/merchandise were being delivered and bogus transactions were being shown to justify credit card usage. With a more active approach towards security by CCA, it would have been possible to ascertain the genuineness of the merchant involved.

d) Learning experiences in Case No. 2

2.15 In the business model followed by IRCTC, the payment is being received through direct debit to internet bank accounts of the customers or through credit cards, whereas the tickets are being delivered to a physical address. In the instant case, the address of a commercial establishment was being used for delivery. There are no safeguards regarding what addresses can be allowed, or for further verification of dubious addresses. The total defrauded amount in this case was not large (only Rs.25,000), but the implications of an organized fraud such as this, on a larger scale, for a nascent public utility service like that of the IRCTC are important for its economic viability and maintenance of public confidence in our national infrastructure, like the Railways.

2.16 According to a report carried by Economic Times in September 2002, transaction volumes in the Indian payment services industry grew 69% in calendar year 2001 to touch Rs 10,935 crore, while card issuance maintained a 30% growth to touch 7.55 million. Card usage levels in India are also one of the lowest in the region. Average credit card usage is at just 11 times a year, indicating huge potential for further growth. With this combination of rising trends in credit card and internet usage and penetration, online credit card frauds are bound to show a sharp upswing.

3. Conclusions

3.1 E-commerce is one of the most promising areas in the applications of internet for the common man. The systems and procedures in this emerging field need to be established with adequate thought, in view of the *in absentia* nature of the transactions. Use of instruments like the credit cards, where the customer is absent, is fraught with risks. There are very few payment gateways in the Country and these are the lifeline for online commerce. The existing levels of checks and balances adopted by the payment gateways for ensuring genuine business on the Net are gravely inadequate. In this scenario, it would be very easy for a dedicated group of criminals to cause serious losses to the economy via the payment gateways.

3.2 Online businesses are reporting more and more frauds on the chargebacks received by them on credit card transactions. This trend is only growing. The possibility that organised crime gangs may exploit the weaknesses and vulnerabilities of the system is very palpable, as this has been the trend the world over. There is need for ensuring accountable systems in online payments, which are of uniform standard the world over, before payment gateways are opened up for e-commerce.

There is also a need for periodical third party information security audits of vital infrastructure like Banks, which is enforceable by Regulatory Authorities.

3.3 As India adopts the modern ways of transacting business through the internet, there is a need to raise awareness adapting the traditional systems and processes to the new paradigm and gear up the law enforcement organisations to meet the new challenges of law enforcement.

Further Reading and Resources:

http://usa.visa.com/business/merchants/fraud_basics_index.html

http://www.faughnan.com/ccfraud.html

http://www.windowsix.com/Controlling_Online_Credit_Card_Fraud.php