E-Commerce Fraud How to Tackle

Mamun Seraji

Bangladesh retail market and service industries are moving towards e-commerce trade, urban millennium generation is getting used to this faster modern way of retail trading. Using ecommerce facility customer can go to a web site, select service or product and make payment using card number and other credentials. Goods/Services are delivered once payment is done.

Bank like BRAC Bank, Dutch-Bangla bank implemented technical infrastructure to act as payment processor and accepting both local and international credit/debit cards (VISA/MasterCard). Providers like SSL-Wireless made e-commerce business much easier for the starters by providing all necessary support like website design, hosting and payment gateway.

However absence of experienced product delivery service providers, less knowledge on e-commerce fraud and related prevention are creating hindrance for the future of this channel in Bangladesh.

E-commerce is a seriously fraudulent channel, if necessary protection and awareness are not taken. Total e-commerce fraud loss for retailers in USA was 3.4 billion USD in 2011 according to CyberSource. On an average approximately 5% of overall e-commerce transaction falls under fraud as statistic says. Card fraud mainly takes place once cards data/card goes to wrong hand.

I am highlighting some *easy to implement* but effective fraud management technique for service buyer and seller, which should be taken into consideration to prevent more than 90% fraud of e-commerce:

From e-commerce buyers standpoint, as customer, if your card is e-commerce enable, do not share plastic card to others (generally we handover the plastic to restaurant boy for making payment), card number, CVV number and expiry date is enough to make a fraud transaction using internet payment portals. When a card is stolen please inform issuing bank as soon as possible for deactivation.

Card's e-Commerce transaction facility must be deactivated in general and feature can only be enabled temporarily by a phone call to issuing bank call center before making transaction.

Please know the website better before placing your card data for making transaction. Hundreds of fraudulent ecommerce sites created a net to capture your card details with fascinating offers.

From e-commerce sellers point of view, use commonsense, take some extra time to review order, read carefully and use your common sense to understand all information user provided are correct. If you feel suspicious, do not process the order and wait until next day.

Address verification: most of the payment gateway/card issuer provides address verification, confirm billing address, delivery address and contact address have synergy or similarity. Matching addresses is a great technique to prevent fraud. If you see a billing address is Bangladesh and delivery address is India, you can consider/park it as fraud transaction for further review.

Free e-mail address : retailers should be careful to entertain request coming from free e-mail address line gmail/hotmail. Most of the fraud request gets generated from these free e-mail requests. Any ISP driven e-mail address /corporate e-mail address is easy to trace, if any case lodged from card owner.

Contact customer/card owner: Contact with card owner via SMS/e-mail or any means to be sure about the e-commerce order before delivery. This is the most effective way to prevent fraud. If required merchants can contact with issuing bank, which can connect merchant to card owner.

IP Address and BIN matching: Store the IP address from where request came. This can be used to match the location of card issued and user making order from. The region of card BIN and IP address can be matched to identify any fraud.

Banks must have separate cell to manage e-commerce fraud, conduct awareness campaign before hand over this feature to customer, enforce mandatory replacement of cards after customer visit to high risk countries of card fraud, ensure proper verification of e-ecommerce service provider by analyzing their nature of business and analysis of customer transaction behaviour.

However, going forward and as technically proven solution - issuing bank has to be triple DES compliant which will force card holder to use password along with card detail for any e-commerce transaction. Like any sophisticated solution- implementation of 3DES is expensive for card issuing bank and none of the issuer in Bangladesh is 3DES compliant as of now. CJ

Writer : SVP & Head of Business Systems Management, BRAC Bank Limited

Feedback : mamunseraji@gmail.com

Intel Inspired Ultrabook Available in Bangladesh

Intel inspired Ultrabook, a new category of mainstream thin and light mobile computers, is now available in the Bangladesh market. Based on the second generation Intel Core processors, Ultrabooks are set to bridge the gap between processing power and portability, promising to be a game changer in the ever-evolving technology market.

Ultrabook
Inspired by Intel

Ultrabooks offer secure computing in sleek portable form factors, with longer battery lives and uncompromising performance. Intel expects that the Ultrabook will be an iconic transformation to mobile computing, just as the introduction of Intel Centrino was a revolution in mobile technology more than eight years ago.

Zia Manzur, Country Business Manager for Intel in Bangladesh said, "The Ultrabook is an emerging new breed of no-compromise computers that will increasingly combine best-in-class performance, improved responsiveness and security in thin, elegant, must-have mobile designs." Currently, there are over 75 designs of Ultrabooks in development worldwide, which is indicative of the kind of popularity and initial demand there is for this category. Ultrabooks from Acer and Toshiba are now available in Bangladesh market, and it is expected that Dell and Samsung Ultrabooks will hit the market soon.

The technical specifications that set an Ultrabook apart from other categories include a design of under 0.8 inches slimness. The Intel Rapid Start Technology gets the system up and running faster from even the deepest sleep, saving time and battery life. Ultrabook devices will offer up to 5 hours of battery life even in the sleekest form factors with some systems delivering up to 8 hours or more for all-day usage. Additionally, the Ultrabook systems are enabled with security features like Intel Anti-Theft Technology and Intel Identity Protection Technology CJ