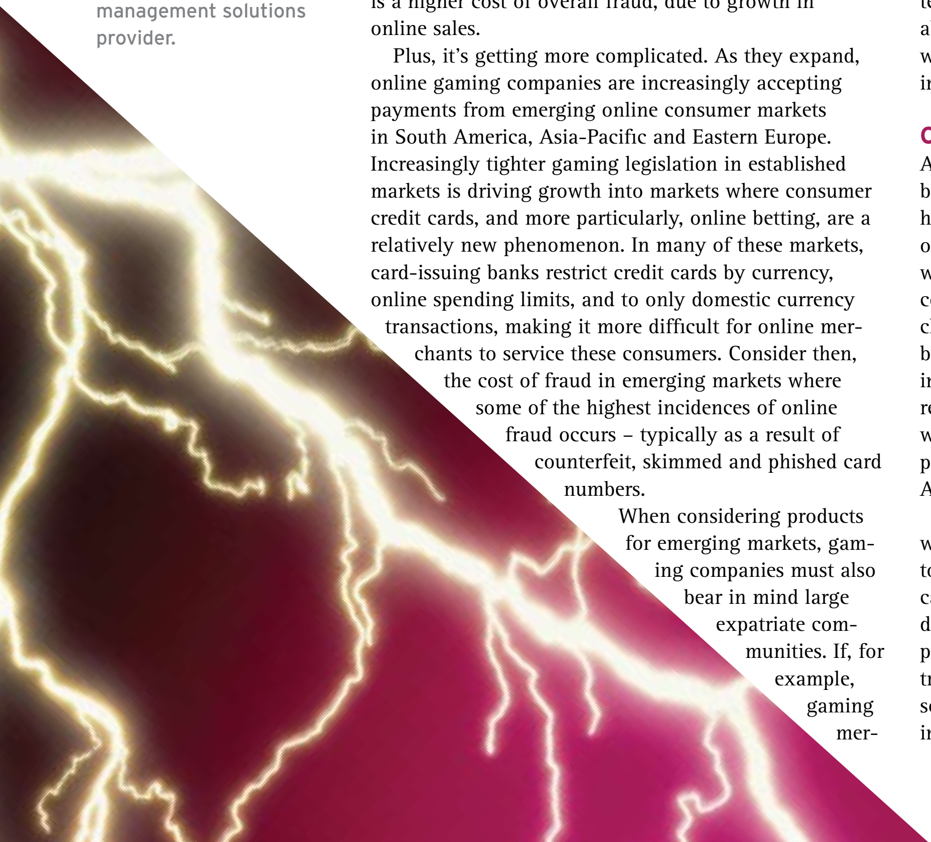
Tricia Lines Hill of First Atlantic Commerce explains how authentication of customers in emerging markets can limit fraud and maximise profits

HARNESSING THE POWER

Tricia Lines Hill is VP, Marketing & Corporate Communications, of First Atlantic Commerce Ltd., a leading international, multi-currency payment gateway and data management solutions provider.



NOTHING RUINS A GREAT processing month like the imminent hangover of chargebacks and transaction fraud. This industry nemesis will never disappear, regardless of how many sophisticated fraud systems, risk-profiling services or phone calls you make to your consumer market. Why? Because you can't predict or control consumer behaviour and the card associations have fostered an online credit card environment of zero liability. According to the card associations, over 75% of all fraud-related chargebacks are represented with two fraud reason codes (23, 83).

CyberSource's ninth annual 2007 *Online Fraud Report* estimates that internet merchants in the US and Canada alone will lose about US$3.6bn in revenue in 2007 due to online fraud, an increase of about 16% from US$3.1bn in 2006. Although in line with sales growth, with the dollar-loss fraud rate holding steady at 1.4% in 2006 and 2007 (according to CyberSource), the bottom line is a higher cost of overall fraud, due to growth in online sales.

Plus, it's getting more complicated. As they expand, online gaming companies are increasingly accepting payments from emerging online consumer markets in South America, Asia-Pacific and Eastern Europe. Increasingly tighter gaming legislation in established markets is driving growth into markets where consumer credit cards, and more particularly, online betting, are a relatively new phenomenon. In many of these markets, card-issuing banks restrict credit cards by currency, online spending limits, and to only domestic currency transactions, making it more difficult for online merchants to service these consumers. Consider then, the cost of fraud in emerging markets where some of the highest incidences of online fraud occurs – typically as a result of counterfeit, skimmed and phished card numbers.

When considering products for emerging markets, gaming companies must also bear in mind large expatriate communities. If, for example, gaming merchants are targeting Asian communities for Pai Gow Poker, they must also consider the large communities of Asian consumers in North America and Europe, who are also interested in playing these games online. Authentication of these consumers is just as critical.

So what is the solution? Authenticating or identifying the customer upfront in advance of a payment transaction is the best bet. There is no point in taking a gamble on a new consumer transaction if you risk not only losing the sale, but also receiving a chargeback, a fine and losing your acquirer in that region. While fraud detection systems and tools are used to identify the probability of risk associated with an online transaction, "They do not guarantee that a fraud will not occur and certainly will never prevent a chargeback from being initiated by the consumer," said Andrea Wilson, CEO of First Atlantic Commerce (FAC).

However, the right blend of fraud management technologies can provide you with enough information about that card transaction to make an informed decision whether or not to proceed with the payment, thus reducing your exposure to fraudulent transactions.

CVV2 Verification

Address verification (AVS) is still widely used for USA billing address confirmations and continues to be a hugely popular initial online screening service. CVV2 or Card Verification Value has picked up momentum, with many issuers declining authorisations if the CVV2 code doesn't exactly match. In 2005, Visa modified chargeback (RC83) to allow merchants to shift liability back to issuers in the event the issuer did not participate in CVV2 verification if presented with the authorisation request. AVS-only as a standalone service is available with or without a payment authorisation and FAC supports $0 (not limited to US$) authorisation requests for AVS zip matching.

Consider combining $1 pre-authorisation requests with CVV2 and AVS data in a pre-screening request to provide some very basic information about the cardholder, including whether the card is valid (if $1 declines there is a problem with the card!); whether the plastic is in the cardholder's possession at the time of the transaction (CVV2 is only located on the signature panel so the logic is that the customer should have the plastic in their possession if CVV2 data matches) and whether the consumer's billing address matches what the issuer has on file.

Location, location, location

Geolocation is an excellent addition to merchants' fraud and risk evaluation solutions. Used to identify the geographic origin of a transaction based on the IP address of the customer's ISP, geolocation data provides specific information about the IP address such as the country, city, region, zip code, time zone and ISP domain name.

It can also be cross-checked with the address verification data that's returned from $0 AVS screening as part of the same transaction request. For instance, if a merchant identifies a consumer IP address as originating in Turkey, yet the credit card billing address data matches a zip address in California, this transaction is suspect and should be investigated further.

IP geolocation is a very important tool for gaming merchants as MasterCard International now requires merchants to identify and store the physical location of their consumers as part of the April 2007 operational compliance changes. Additionally, licensing agencies and regulatory organisations who enforce territory compliance can use IP geolocation to ensure merchants are not violating compliance with the Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA) if this so applies to their specific licence regulations. "Typically, most online geolocation software providers are unable to bundle traditional payment authentication services with IP geolocation data requests in order to provide this level of cross-referencing. This is what makes FAC's solutions unique in the market. We have combined innovation with flexibility and have created a suite of solutions that improve transactional risk profiling," adds Wilson.

Safe and secure

3-D Secure™ is currently the single-most-important fraud-prevention service offered today by the card associations for online merchants. Available in the consumer's local domestic currency and language of the bank issuer, it enables gaming companies to implement Verified by Visa and MasterCard SecureCode™ in all regions, and more particularly emerging markets such as Asia, South America or Eastern European markets.

With the 2007 MasterCard changes in chargeback liability shift rules for 'attempted' SecureCode transactions, both Visa and MasterCard now support chargeback liability shift in Asia/Pacific, LACR, CEMEA and Europe for qualifying attempted 3D Secure™ transactions (for RC 23 and 83). What's important to understand is that liability shift is based on the merchant's attempt to verify the consumer or the issuing bank – not on whether the cardholder is actually enrolled in Verified by Visa or MasterCard SecureCode™.

FAC has taken 3-D Secure™ solutions one step further and allows merchants to perform Verified by Visa and MasterCard SecureCode™ as a standalone solution. FAC is certified to support local currency 3-D Secure™ in LACR, Europe, and CEMEA regions. This allows merchants to know in advance of full payment authorisation whether they will have a chargeback re-presentment right based on the 3-D Secure™ response code, and when the full payment transaction is subsequently processed through a 3-D Secure™ acquirer.

Data sharing

Other consumer authentication solutions include data sharing, a practice by which companies contribute and connect to a pool of shared data for mutual risk analysis and benefit. Companies who review shared data in real-time in advance of a payment transaction can identify habitual chargeback offenders and declined card numbers to better evaluate fraud risk based on collective industry experience. Top gaming and sportsbook operators in the industry have signed on as members of data sharing fraud-fighting communities, such as ETHOCA, in a collaborative effort to reduce industry fraud.

> "We have combined innovation with flexibility and have created a suite of solutions that improve transactional risk profiling"

Leading the Game

If you are looking to centralise your security, risk and payment solution efforts, you need to look at what existing payment solutions providers can provide to you as a suite of solutions so you do not have to implement individual interfaces and services across multiple vendors. First Atlantic Commerce can customise your pre-authentication solutions after reviewing business and operational objectives. We realise no two businesses are ever the same and a shrink-wrap solution simply does not fit all business models. FAC can transform your transactional risk challenges into business opportunities by providing you with the tools you need to cut fraudulent activity, reduce chargebacks and increase your profits.