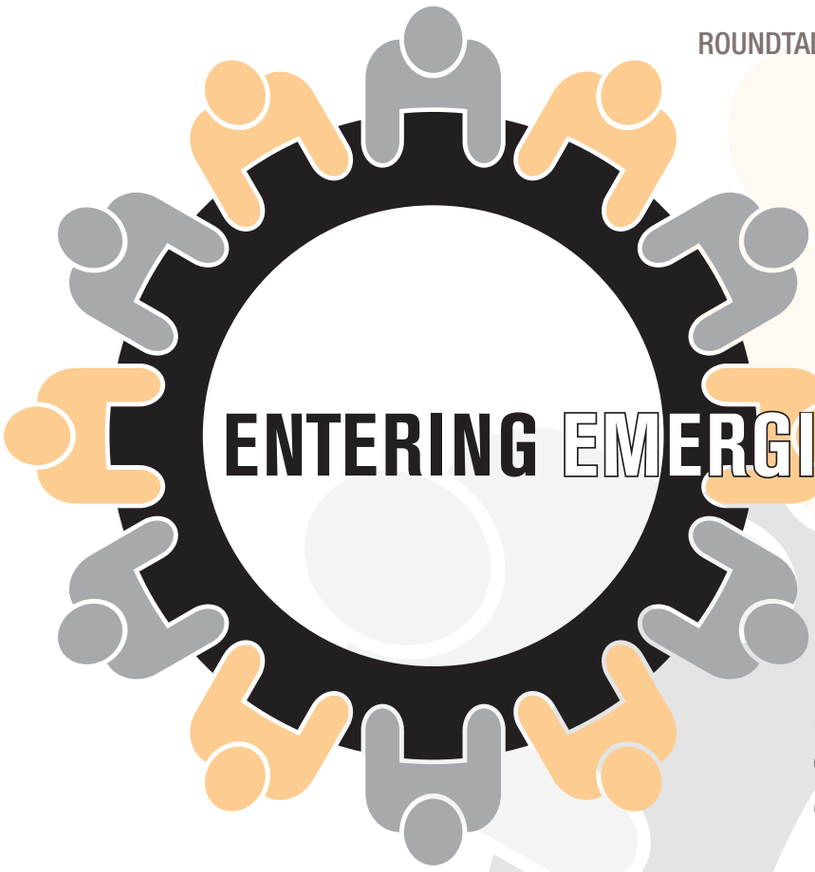

ENTERING EMERGING MARKETS

How do operators target the right customers, and protect themselves entering emerging markets?

TRICIA LINES HILL, VP MARKETING & CORPORATE COMMUNICATIONS, FIRST ATLANTIC COMMERCE

As the gaming industry continues to adjust to US legislation changes, and grow outside of its traditional markets, it looks to the emerging economies for expansion.

Gaming suppliers and operators are turning to new markets every day to grow their business, but as they enter different markets, they find themselves faced with even higher levels of online fraud than in traditional markets. In fact, in our experience as an online payments and fraud solutions provider, we have found this "Know Your Customer" issue to be the one consistent gripe amongst operators in new regions.

Merchants must be aware that targeting customers in emerging markets requires a different overall online risk management strategy. The key is for gaming operators to protect themselves from criminal attackers ahead of customer acquisition and transaction processing (thereby avoiding chargeback losses).

Since fraud levels are inherently higher in the Latin American Caribbean market and in Asia, for example, merchants have to know who they are dealing with before the players place their bets. They have to electronically authenticate their customers during the registration process, and there are many ways to do so.

CUSTOMER AUTHENTICATION

Firstly, operators should do basic credit card electronic vetting including Address Verification Services (AVS) and CVV2 match checks before a payment authorisation request is performed. CVV2 is mandated by Issuers worldwide and there is provision for CB liability shift under RC83 for non-response to a CVV2 match request by an Issuer.

If the consumer is from North America, an AVS-only or AVS+CVV2 data check should be performed (again without payment authorisation). AVS provides some degree of comfort that the consumer receives the credit card bill to a home address or that a home address with a zip/postal code is registered with the bank. If the AVS data matches and so does the CVV2 value, there is more confidence that the cardholder is legitimate and has possession of the physical plastic. This, of course, is not an indication of their ongoing chargeback habit, but rather a confirmation that the card is not stolen or counterfeit when they register.

Another fast method of confirming cardholders is via Cardholder Account Confirmation. It's a transaction pre-screening solution that validates a cardholder's card by processing random micropayment transaction amounts with a unique cardholder descriptor at the account registration process.

The cardholder must verify the settled transaction and enter the amount charged by the merchant at the site, which validates that the consumer is actually authorised to use the credit card account. Once the card account is confirmed by the settled transaction and verified by the customer, the balance of the transaction, or further transactions, can be charged and processed.

Implementing 3-D Secure™ payer authentication solutions (VBV and SecureCode) in advance of a full payment authorisation also provides information on the implementation status of the Issuer's BINs, as well as the cardholder's enrolment status. This is an important tool in identifying your chargeback liability shift rights before allowing a consumer to use a registered credit card at your site.

Ideally, a merchant should combine all of the above solutions for the most advanced consumer authentication screening. They provide especially good layers of upfront fraud protection for unknown consumer groups in emerging card-not-present markets like South America and Asia/Pacific.

FAC can provide all of these solutions to merchants as a stand-alone service or as part of a payments package, which means that merchants do not have to switch gateways to get access to the service.

JOHN PETERSON, BUSINESS DEVELOPMENT MANAGER, GLOBALCOLLECT AMERICAS

With access to the Internet, online markets became global. As a driver of customer acquisition, entering emerging markets has become a core strategy to fuel business growth. So how can you, as an online merchant, ensure getting the right support to grow your market share in emerging markets?

A key success factor for customer acquisition in emerging markets is offering familiar and popular local payment methods. It helps to know that online purchasing patterns reflect those displayed by consumers for offline purchases. However, online payment methods can be as diverse as, (1) converting cash to a usable online payment format by using pre-paid cards or electronic PIN invoices, (2) bank transfers using mandates or real-time push payments, and (3) international and domestic credit and debit cards.

Identifying the right payment methods for potential customers while minimizing the risk of fraud is a challenge for all e-commerce transactions, so it becomes crucial to offer preferred local payment methods in emerging markets. Brian Nagel summarized how the fraud environment has changed in a press release after

Operation Rolling Stones lead to several arrests for Internet merchant fraud.

"Cyber-crime has evolved significantly over the last two years, from dumpster diving and credit card skimming to full-fledged online bazaars full of stolen personal and financial information." Brian Nagel, Assistant Director, US Secret Service.

Some highlights of the potential threats a merchant may face, both at home and in emerging markets include:

- Madrid was the city with the most bot-infected computers, accounting for 14 percent of the total percentage worldwide.
- Bank accounts were the most commonly advertised item for sale in the underground economy, accounting for 22 percent of all items.
- The most commonly 'phished' high-level domain is .com, accounting for 44 percent of all 'phished' websites.

TABLE 1: MALICIOUS ACTIVITY BY COUNTRY

Current Rank	Previous Rank	Country	Current %	Previous %	Bottom Rank	Command-and-control	Phising websites	Malicious code rank	Spam Zombies rank	Attack origin rank
1	1	USA	31%	30%	1	1	1	1	1	1
2	2	China	7%	10%	3	5	2	2	4	2
3	3	Germany	7%	7%	2	2	3	7	2	3
4	4	UK	4%	3%	4	19	15	9	9	4
5	7	Spain	4%	3%	4	19	15	9	9	4
6	5	France	4%	4%	8	14	6	11	7	6
7	6	Canada	3%	4%	13	3	5	4	35	7
8	8	Italy	3%	3%	5	10	11	10	6	8
9	12	Brazil	3%	25	6	7	13	21	3	9
10	9	South Korea	2%	3%	15	4	9	14	13	10

Source: Symantec Corporation

TABLE 2: BREAKDOWN OF GOODS & SERVICES AVAILABLE FOR SALE ON UNDERGROUND ECONOMY SERVERS [28]

Current	Previous	Goods & Services	Current %	Previous %	Range of Prices
1	2	Bank accounts	22%	21%	$10-$1000
2	1	Credit cards	13%	22%	$0.40-$20
3	7	Full identities	9%	6%	$1-$15
4	N/A	Online auction site accounts	7%	N/A	$1-$8
5	8	Scams	7%	6%	$2.50/week-$50/week for hosting, £25 for design
6	4	mailers	6%	8%	$1-$10
7	5	Email addresses	5%	6%	$0.83/MB-$10/MB
8	3	Email passwords	5%	8%	$4-$30
9	N/A	Drop (request or offer)	5%	N/a	10%-50% of total drop amount
10	6	Proxies	5%	6%	$1.50-$30

Source: Symantec Corporation

The global Internet economy is accompanied by a movable underground economy, used by criminals and organized crime to trade in or barter stolen information and services. This information includes government-issued identification, credit cards, credit card verification data, debit cards, personal identification numbers (PINs), user accounts, email address lists and bank accounts. With the help of integrated fraud prevention tools and systems, Payment Service Providers track fraud usage patterns across the Internet to minimize the risk for consumers, merchants and financial institutions. The benefit to merchants is that they can use these systems to maximize customer conversion rates while minimizing fraud.

The two tables (table 1 and 2) from Symantec's report on Global Internet Threats to e-commerce illustrate malicious activities by country and the range of stolen data and goods available via the underground economy.

To mitigate these risks, GlobalCollect's scalable Fraud Screening Service features a range of integrated fraud reduction tools from renowned partners to maximize transaction safety prior to payment authorization. These include customised business rules, neural networks to detect suspicious behaviours and patterns, IP geolocation data to determine the real-world location of a web visitor and a pre-check for fraudulent use of credit cards known to be linked to recognized gold farmers.

ALESSANDRO HATAMI, MANAGING DIRECTOR, PAYPOINT.NET

The emerging markets of Eastern Europe and Asia are the new battleground for online gaming providers. As their people become more prosperous and high-speed Internet access becomes more readily available, demand for online gaming is booming. What's more, many emerging economies – particularly in Asia and South America – look set to be spared the worst ravages of the credit crunch. In other words, they present real growth opportunities amid an otherwise bleak economic landscape.

That's the good news. The flipside of the emerging markets opportunity is greater risk, with fraud, unsurprisingly, the biggest concern. What is more, the regulatory environment for gaming can vary significantly from one territory to another. This not only adds to the complications of running a global online gaming business, it also makes it far harder to adopt common policies for managing fraud. Whilst there is a wide range of technology solutions available, which facilitate every key risk management process, successful operators will combine these powerful capabilities with intelligence about every territory they operate in.

Only a few years ago, the data providers who support age and ID verification data procedures – commonly referred to as know your customer (KYC) might only have covered a handful of western markets. Today, coverage is virtually global. The quality of the data on offer, though, can vary: coverage of Western markets is very good, and in Eastern Europe the situation is improving. However, Asian and South American markets present greater problems. In many countries, it is not really possible to rely on third-party data. And the gaps in the KYC process present ripe opportunities for fraudsters to exploit.

Minimising online fraud is, of course, the reason why KYC safeguards exist. Gaming sites which experience more than a tiny percentage of fraudulent transactions risk attracting the attentions of the card companies; persistent offenders can be blacklisted altogether. Whilst KYC can be very effective at preventing fraudsters signing up, the right payment solution can actually stop them taking part at all. The most advanced payment platforms use real-time fraud management tools which can check card details across literally dozens of fraud criteria – not just address verification and CVV cross-matching, but actually comparing the physical location of the customer with the address of the cardholder.

This real-time intelligence is important – it allows operators to wave through legitimate customers with little interruption to their experience, whilst enabling them to identify and halt potential fraudsters before any money changes hands. The most important step is to develop the fraud detection rules which help operators catch out the criminals, whilst building a loyal (legitimate) customer base at the same time: providers need to focus on building their businesses – not doing detective work.

Striking the right balance between rigorous risk management and the need to build a successful emerging markets strategy, relies, more than anything else, on a close understanding of the realities of every new marketplace. Obviously, the best way to do this is to hire local management who understand the intricacies of their market inside-out. However, this can take time. Meanwhile, providers could go far worse than talk to their existing online payments and KYC providers, whose global experience will go a great way to help them implement the right policies for future success.