

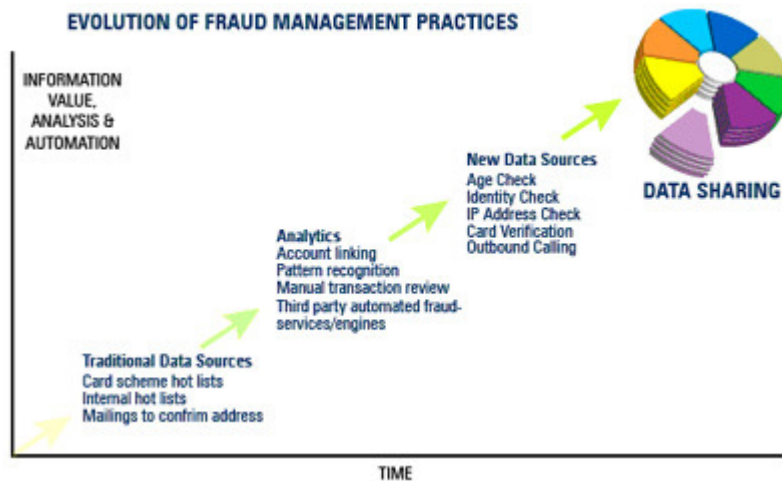


Monday, August 6, 2007

The Evolution of Fraud Management in eGaming

by Andre Edelbrock

The online gaming entertainment industry has long been a target for fraudsters in attempting to gain through fraudulent activities. Fraud continues to negatively impact the bottom line of companies operating in this space, and impacts a number of areas. Chargeback rates, wrongly rejected transactions, manual review costs and fraud management costs all need to be balanced effectively in order to maximize revenue and all important profit. Fraudsters work at a lightning pace and as a result fraud management practices have continued to evolve in order to keep pace.



The Early Days

Traditional fraud management practices focused revolved around both internal and external data sources. Operators relied on their own list of "blacklisted" card numbers to verify each transaction. When available, negative lists supplied by card schemes were also incorporated into the review process. Operators also checked information given by contacting customer by phone and also confirming address details through mailings. This was both an expensive and a time consuming process--often resulting in customer inconvenience.

Introducing Analytics

Many online operators progressed to setting up internal analytics groups. These groups focused on the transaction data within the operator and would continuously monitor for patterns that potentially indicated fraud. Many operators also engaged the fraud management services of third party providers, sometimes provided by payment processors. If a transaction was deemed potentially risky, it was often referred for manual review to the fraud group. They would conduct numerous manual checks to validate the transaction. Analytical strategies helped in identifying

risk but were expensive to scale with business growth. Often operators frequently refused potentially good transactions in order to keep both manual review costs and the fraud rate low.

New Data Sources

New data sources started to emerge that enabled operators to verify the age, identity and in some cases the location of the customer. While not available in all geographies they offered improved protection against fraud. More recently, following the success of the chip and pin protection in the offline retailing sector, similar attempts are being made to introduce these fraud protections online. These do not however cover all customer interactions, payment types or geographies.

Data Sharing - The Future

All of the previous fraud management tools have developed and evolved as fraud became more advanced. These approaches, however, focus on operators managing fraud on an individual basis. In addition, they also focus on potential indicators of fraud. What are missing in the battle against fraud are details about actual occurrences of fraud and taking it one step further, suspected unwanted activity. Data sharing provides this vital missing piece by allowing operators to share their collective experience in a safe, secure and real-time manner. *Data sharing is the practice by which companies contribute and connect to a pool of shared data for mutual benefit.*

Data sharing does not replace the previous forms of fraud management but actually compliments and enhances them. Fraudsters operate on a global stage and have colluded for years. Fighting online fraud can be achieved by cooperation amongst operators rather than competition.

FROM THE EDITOR: [Tell us what you want to read about in IGN.](#)

About the Author

With more than 10 years experience in a variety of challenging roles, Andre Edelbrock is a leading expert in online payments and fraud management. Prior to joining Ethoca in 2005, Andre headed the department responsible for all international e-cash services and operations, and product management at CryptoLogic – (NASDAQ: CRYP, TSX: CRY, LSE: CRP), one of the prominent gaming and payment solution providers in the Internet gaming industry. In late 2000, he spent two years with Procuron, an Internet B2B marketplace start-up founded by Bell Canada, CIBC, Scotiabank and Desjardins. Andre has international business experience managing multi-jurisdictional operations with many years of experience as a management consultant, with a majority of that time spent with Deloitte Consulting (Toronto office) and IBM. He holds an Honours Bachelor of Science degree in Systems Design Engineering from the University of Waterloo. Andre may be reached at andre@ethoca.com.