

**INTERVIEW:**

BattleClinic's Chris Condon Shares Strategy on Preventing Gaming Fraud and Chargebacks

Tell us about BattleClinic and your background in the gaming industry.

I'm Chris Condon and I founded BattleClinic in 2001. My background includes 18 years in corporate organizational development, especially around building learning games. It comes in handy when designing new player guides, tutorials, and tools that help gamers learn their favorite MMOs.

BattleClinic is an award-winning independent game support site that we've been running continuously for 8+ years. We build publisher-sanctioned tools and guides and provide these free to players in order to drive virtual items and game timecode sales. We do this in partnership with the publisher; we're not gold farmers. In 2008, we sold \$1.2 million gross in authorized virtual timecode sales. We currently support and are authorized resellers for EVE-Online published by CCP and City of Heroes published by NCSoft. We are building support for Jumpgate Evolution published by Codemasters, Black Prophecy developed by Reakktor Media, Star Trek Online developed by Cryptic Studios, and Galaxy Online & Freesky Online published by IGG. We reach a broad demographic including adult gamers with extra disposable income.

Describe your first major encounter with online fraud and chargebacks.

CC: When we began offering game timecodes for EVE-Online, we put some fraud prevention in place like order limits, but we didn't experience significant losses and didn't think much about anti-fraud controls.

That all changed one day when the email inbox suddenly filled up with chargeback notices. We took additional preventative measures, but losses mounted.

“ We've seen a 95% reduction in our chargeback rate in 8 months. ”

Chris Condon
Chief Executive Officer,
BattleClinic

Chargebacks on virtual items hurt: there's no way to recover a code or an in-game item, and each can be used minutes after delivery. Our chargeback rate shot up to almost 15% in 30 days and we were in danger of losing our merchant services accounts altogether.

We studied the transactions. There were patterns to the fraud and there was clear indication that the fraudster was reacting to our measures. For example, at first the fraudulent orders seemed to originate in Turkey. We blocked those IPs, which resulted in a few complaints from legitimate customers. A month later, chargebacks returned—this time from customers in Greece. Then Italy, then France. As we reacted, other patterns emerged: fraudulent transactions all came from email domains like mail.com, comic.com, wallet.com, and bikerider.com. Or we'd get rotating patterns: in one month, a few orders from New York, followed by a few from Texas, and then a few from California. Next month, different customer names, same regions.

How did this impact your business and what did you do to stop it?

CC: We bore significant direct costs, and incalculable hidden cost. We kept manually adjusting our fraud prevention measures, which invariably blocked legitimate orders, cost goodwill, damaged our reputation, and more. Account approvals slowed, service levels suffered, and viable customers walked away. Ouch.

Gamers are extremely sensitive to service levels and delivery speed. We couldn't afford to upset them with intrusive phone calls to verify their purchase. Nor could we afford to make them wait days or weeks to ensure the payment cleared. Gamers want their stuff now! We needed real-time fraud protection that didn't interrupt or slow fulfillment. And as volume increased, we didn't want to bottle-neck anything either.

After \$20,000 in direct losses and who knows how many lost opportunities, we just couldn't stay in reaction mode. We went looking for a proactive solution and found iovation. We were drawn to the idea of sharing fraud profiles with other subscribers. Plus, the fraud checking is done in real time and it scales to volume which eased my concerns about customer impact. Implementation was straightforward.

Since implementing iovation's fraud protection service, at what rate has fraud decreased?

CC: Within the first month of implementation, we caught one person running eight accounts, another running seven accounts, and many running three accounts. We blocked hundreds of attempts to create new fraudulent accounts in the months that followed. The attempts became more random and more intense for a while, and then dropped dramatically. Preventing half the fraud attempts each month pays for the system; we've seen a 95% reduction in our chargeback rate in 8 months.

In the world of on-line MMO gaming, RMT (Real Money Trading) website operators will gather items inside the game and sell them outside of the game, depriving the publisher of revenue. Some defraud the publisher-authorized timecode and virtual item resellers to feed the RMT market. Since RMT is such a huge problem for the game publisher and the reseller, sharing a fraud database makes perfect sense. Since our business model is to help drive more subscriptions to MMO games, keep the players playing longer and buying more authorized virtual goods, we see nothing but upside in how iovation's fraud protection service works for us.

To learn more about iovation ReputationManager™ and how it helps organizations fight online fraud and abuse, visit www.iovation.com.



iovation Inc.

111 SW 5th Avenue, Suite 3200, Portland, OR 97204

+1.503.224.6010 tel | +1.503.224.1581 fax

www.iovation.com