The Financial and User Experience Effects of Online Game Fraud

Authors Removed for Review

Extended Abstract

Game companies have a stronger digital presence today than they had even half a decade ago, seeking to create larger, connected systems where players can play games, interact with other players and purchase content. With the raise of digital distribution services, micro-transactions, early access and downloadable content, game companies have direct lines to their players when it comes to delivering digital products. In turn, these direct lines means game companies become liable for and susceptible to nefarious actions that often plague other commercial entities, namely fraud.

Online fraud has increased for many games and game services as the value of online game environments has increases. Persistent game environments found in genres such as MUDs and MMOs have been available for decades and allow users to generate capital (whether financial, social or cultural), or otherwise value, over time (Consalvo, 2007; Dibbell, 2006; Frieling, 2006; Heeks, 2010; Shen, Monge, Williams, 2012). Game companies and platform developers (e.g. console manufacturers) have turned to similar tactics to create persistent value for players. They are moving away from providing individual game experiences to a 'games as a service' model where persistent data systems extends a player's online game identity across any number of games, creating further value and ownership for players (Medler, 2011). With game companies working to increase the value of their games and services, and players equally placing value in their gaming identities, it stands to follow that fraudulent behavior begin to emerge as the real world value that exists within games increases.

Fraud occurs within games when real world currency can be extracted from a game, meaning in-game value turns into real world value. Fraud that occurs using real world payment methods and systems equate to payment fraud, for example fraudulent accounts using stolen credit cards to purchase content ((, 2011;

Patidar and Sharma, 2011). In the case of payment fraud, fraudulent players initially extract value from a game by making fraudulent purchases, where the funds cannot be collected, and can extract further value from other players by selling the content purchased. Payment fraud has direct financial impact on a game company as the fraudulent players commit fraudulent transactions (which the game company must pay fees on top of the lost transaction amount) and in-direct impact as a fraudulent player often sells content they fraudulently purchased to other players.

In addition to payment fraud there is also game fraud which bypasses real world payment methods but still extracts real world value from in-game content. Gold farming is one of the more well-known types of game fraud where players use various methods to acquire large sums of in-game resources/money that is then sold for real world currency (Nardi and Kow, 2010). Account take over (ATO) (Castell, 2013) is the other major game fraudulent practice where fraudulent players take control of a player's accounts without the player's knowledge, using the accounts for spamming, gold farming or even selling the whole account. While game fraud practices do not directly involve using false real world payment methods, as payment fraud does, game fraud practices alter a game's economy, increase customer service problems and negatively affect the player experience of a game.

In order to combat both payment and game fraud a combination of approaches is necessary due to the fact that fraudulent activities affect game teams financially and alters the player experience. Research around gold farming practices, for instance, tend to focus on data mining approaches for searching and identifying accounts committing game fraud (Ahmad et al. 2009; Keegan et al., 2010; Roy et al. 2012). While the methods used to find gold farmers are important to test and implement, the methods only tackle the problem of identifying a specific type of player committing a specific type of fraud. Other issues related to customer experience, database engineering, financial tracking, risk system development, etc. are needed to devise a holistic approaches to combating fraud in games.

In this article the authors explores what fraud means for game companies and players. The holistic problem of combating fraud requires game companies to direct a number of different disciplines towards

a common goal of monitoring, analyzing and acting upon fraudulent players. Additionally, how legitimate players experience the effects of fraud is equally important as they expect a level of security and fairness to exist within their game environments. With these topics in mind the authors cover:

- Key terms and concepts related to fraudulent behavior in games.
- Current approaches to fraud prevention including risk management systems and game analytic methods.
- Examples of how a combination of game development and operations teams work together to protect players.
- Ways in which players are affected by fraudulent activity and fraud prevention system.
- Future directions towards building better fraud detection systems.

References

Ahmad, M. A., Keegan, B., Srivastava, J., Williams, D., & Contractor, N. (2009, August). Mining for gold farmers: Automatic detection of deviant players in mmogs. In Computational Science and Engineering, 2009. CSE'09. International Conference on (Vol. 4, pp. 340-345). IEEE.

Castell, M. (2013). Mitigating Online Account Takeovers: The Case for Education. Retrieved from: https://www.frbatlanta.org/documents/rprf/rprf_pubs/130408_survey_paper.pdf

Consalvo, M. (2007). Cheating: Gaining Advantage in Videogames. MIT Press.

CyberSource (2013). 2013 Online fraud Report. 14.

Dibbell, J. (2006). Play money: Or, how I quit my day job and made millions trading virtual loot. Basic Books.

Frieling, J. (2013). Virtual goods in online worlds: basics, characteristics and monetization. In GI-Jahrestagung (pp. 3097-3107).

Heeks, R. (2010). Understanding "Gold Farming" and Real-Money Trading as the Intersection of Real and Virtual Economies. Virtual Economies, Virtual Goods and Service Delivery in Virtual Worlds. 2(14).

Keegan, B., Ahmed, M. A., Williams, D., Srivastava, J., & Contractor, N. (2010, August). Dark gold: Statistical properties of clandestine networks in massively multiplayer online games. In Social Computing (SocialCom), 2010 IEEE Second International Conference on (pp. 201-208). IEEE.

Medler, B. (2011). Player dossiers: analyzing gameplay data as a reward. Game Studies Journal, 11(1).

Nardi, B., & Kow, Y. M. (2010). Digital imaginaries: How we know what we (think we) know about Chinese gold farming. First Monday, 15(6).

Ogwueleka, F. N. (2011). Data mining application in credit card fraud detection system. Journal of Engineering Science and Technology, 6(3), 311-322.

Patidar, R., & Sharma, L. (2011). Credit Card Fraud Detection Using Neural Network. International Journal of Soft Computing and Engineering (IJSCE) ISSN, 2231-2307.

Roy, A., Ahmad, M. A., Sarkar, C., Keegan, B., & Srivastava, J. (2012, September). The ones that got away: False negative estimation based approaches for gold farmer detection. In Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom) (pp. 328-337). IEEE.

Shen, C., Monge, P., & Williams, D. (2012). Virtual brokerage and closure: Network structure and social capital in a massively multiplayer online game. Communication Research, 0093650212455197.

Woo, K., Kwon, H., Kim, H. C., Kim, C. K., & Kim, H. K. (2011, August). What can free money tell us on the virtual black market?. In ACM SIGCOMM Computer Communication Review (Vol. 41, No. 4, pp. 392-393). ACM.