Online Fraud and the part it plays in Cybercrime

OWASP
The Open Web Application Security Project

Alex Doroftei
adoroftei@ea.com

Fraud & Risk Supervisor
Electronic Arts

What is Online Fraud?

Definition

Online fraud is defined as the **use of deception by an individual or group of individuals**

using an online medium with the intention of obtaining an advantage for himself or herself or for a third party or parties, avoiding an obligation, or causing loss to another party.

OWASP
The Open Web Application Security Project

Example of Fraudulent Activity

Fraudster obtains credit card information from underground online user group

Fraudster phishes a legitimate PayPal account via e-mail

Fraudster purchases product online using fraudulent/stolen account

Fraudster resells product on their 3rd party sites or black markets at a reduced price

Silk Road
anonymous marketplace

The legitimate card holder issues a chargeback through their bank.

Company loses sales revenues when legitimate card owner requests a chargeback on their account

Fraudster repeats process using additional fraudulent accounts

OWASP
The Open Web Application Security Project

Education in the cybercriminal world

Fraud-as-a-Service (FaaS) strives to resemble legitimate business models, fraudster trade schools further offer 'job placement' for graduates through their many underground connections with other experienced criminals. Interestingly, some of the "teachers" go the extra mile and vouch for students who show "talent" so that they can join the underground communities they would otherwise not be able to access.

OWASP
The Open Web Application Security Project

Education in the cybercriminal world

Courses can contain and not only:

- Beginners' cybercrime classes (Price per lecture 2,500 Rubles - $75 USD)
- Courses in card fraud (Price per course 2,500 Rubles - $75 USD)
- Anonymity and security course (Price 3,300 Rubles - $99 USD)
- Mule Herding Course (Price 1,500 Rubles -$45 USD) per scenario)
- One-on-one tutorials and consultations (Price 2,000 Rubles - $60) per hour)

Fraud circles / rings

Instances of cyber fraud could be distinguishes into two different “models" of cyber fraud networks that exist.

The first is a loosely-affiliated model of individuals or small groups with no one in charge.

The second “model" functions more like a large scale criminal organization with a centralized structure

Source : ThreatMetrix

OWASP
The Open Web Application Security Project

Why is Fraud Management important?

- **Loss of revenue**

  Revenue loss arising from chargebacks

  Revenue loss resulting from paying commission to hosting providers for transactions generated even if chargebacks are later issued

  Revenue loss from lost sales due to existing black market for online goods

- **Incur fines and fees**

  Chargeback penalties are levied by card brands and payment aggregators.

Why is Fraud Management important?

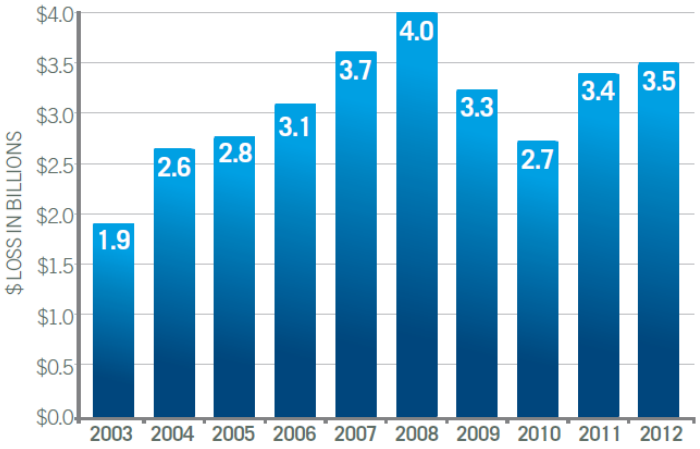
- **Loss of card brand processing rights**

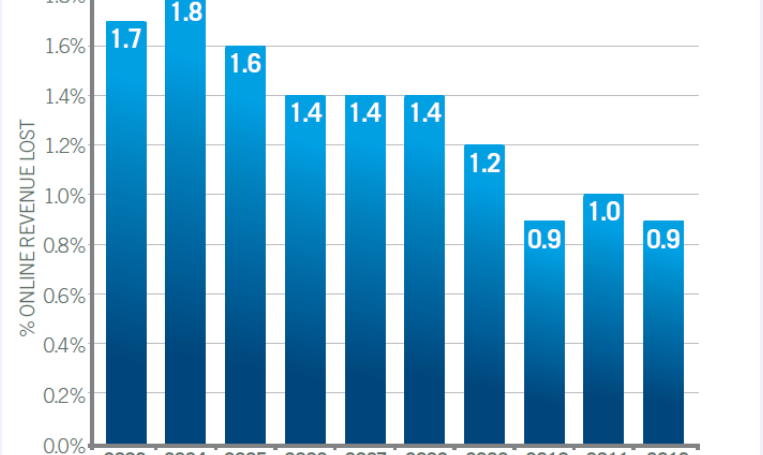
  Card brands may revoke processing rights due to continual high chargeback rates

- **Brand reputation**

  A high fraud rate will adversely affect your relation with its customers and its partners. For example, fraudulent users spamming/gold farming the community causes poor game experience for legitimate players and in turn impacts your games reputation.

Why is Fraud Management important?





(CyberSource 2013 Online fraud report)

OWASP
The Open Web Application Security Project

A few thoughts

- Understand your business model and how fraud can be perpetrated.
- Understand the payment method and region your are releasing your product into.
- Partner with your vendors and other internal teams to help support your fraud management initiatives.
- Get involved with organizations and groups against fraud.

While network security teams focus on perimeters and firewalls, cybercriminals are finding easy access through the business front door with stolen credentials, unprotected devices, and compromised credit cards

Question & Answers