



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



OWASP

The Open Web Application Security Project

What is Online Fraud?



Definition

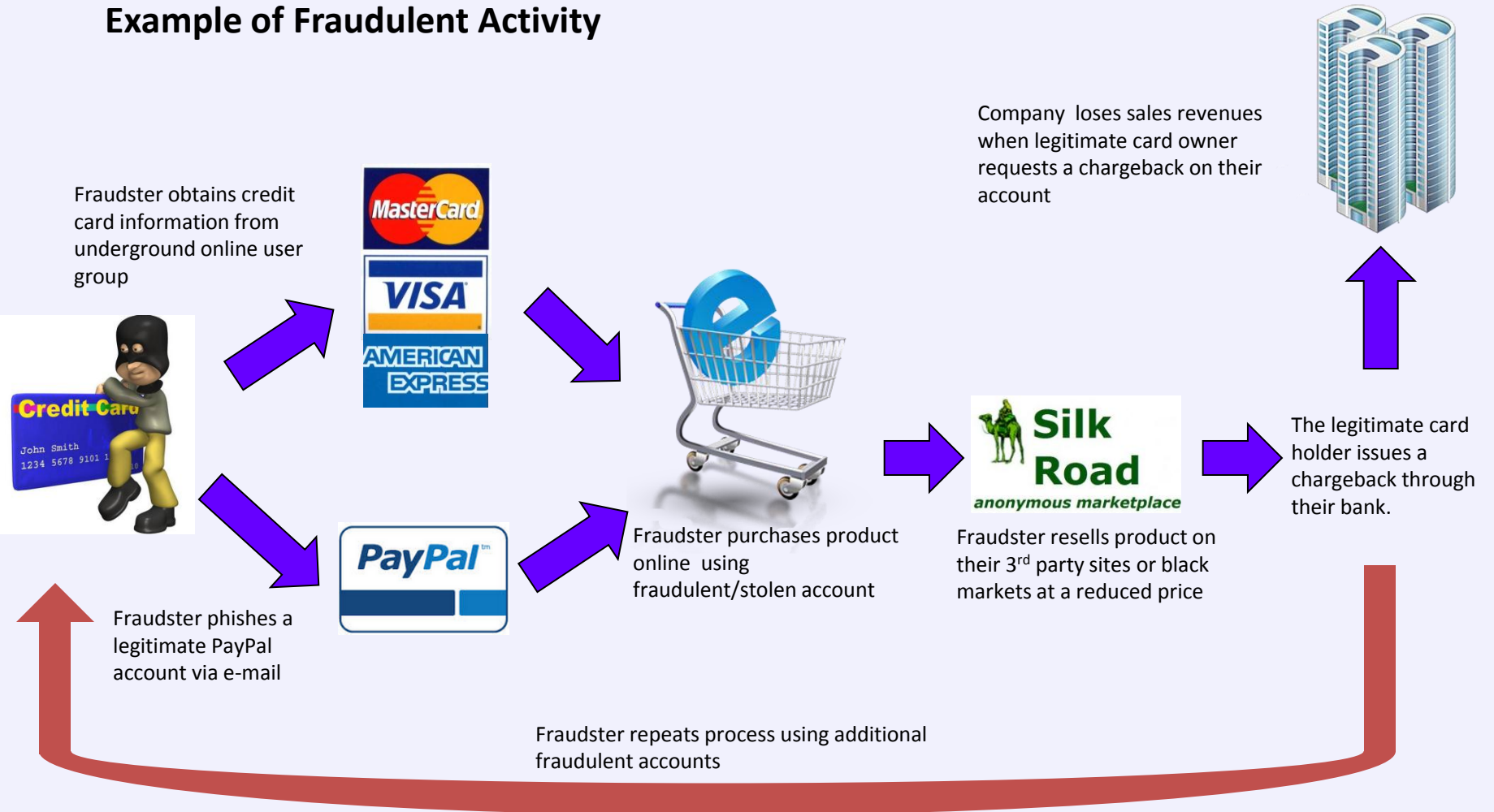
Online fraud is defined as the **use of deception by an individual or group of individuals using an online medium with the intention of obtaining an advantage** for himself or herself or for a third party or parties, avoiding an obligation, or causing loss to another party.



OWASP

The Open Web Application Security Project

Example of Fraudulent Activity





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)



OWASP

The Open Web Application Security Project

DANA BREACH accesses the bank accounts full of stolen funds that Work-at-Home Wally set up for her.

She also writes software that compromises bank accounts. The software intercepts user login sessions, enabling Dana to access their accounts.

Finally, Dana sells her software to **Sam Spam**.



SAM SPAM purchases scripts from Dana that use fake information to register for social networking sites. He then auto-creates many fake social profiles.

Sam uses the fake profiles, as well as phony Facebook apps, to send spam emails with links to viruses that infect the recipients' devices.

Once Sam gets paid for every virus that's installed, he passes along the credentials from the infected computers to **Connie Compromise**.



WORK-AT-HOME WALLY receives the stolen goods from Hugo and repackages them for **Dana Breach**. He also transfers money to other bank accounts that Dana can access.



CONNIE COMPROMISE uses Sam's stolen credentials from virus-infected computers. She is thrilled about the recent data breaches by organizations like LuzSec and Anonymous—they make her job much easier.

Connie visits compromised online retailers and steals customers' credit card information by using SQL injection attacks. She gathers customers' card numbers and personal information, and sends it to **Frederick Fraud**.



NOTE: Work-at-Home Wally was unknowingly recruited into this fraud network through a work-at-home scheme.

Working overseas, **HUGO HACKER** uses Frederick's validated, stolen credit cards to tunnel through compromised computers and place online orders for luxury goods. Websites won't detect the invasion because Hugo's IP address mirrors that of the compromised computer.



FREDERICK FRAUD is a part-time fraudster. He verifies the validity of Connie's stolen credit cards by sending out scripts to target gaming and gambling sites for the purchasing of virtual currencies.

The instant transactions are approved immediately. Frederick tests the virtual currencies, using very little of the available funds, and passes the info on to **Hugo Hacker**.



Hugo visits online hacker forums, where he pursues information about compromised devices that correspond to his batch of stolen identities.

He uses a drop-ship to send the stolen goods to his cousin in the U.S., **Work-at-Home Wally**.

Fraud circles / rings

Instances of cyber fraud could be distinguished 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.



OWASP

The Open Web Application Security Project

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.

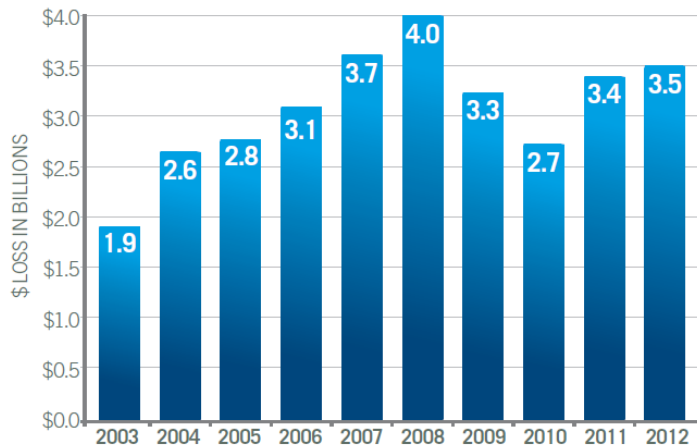


OWASP

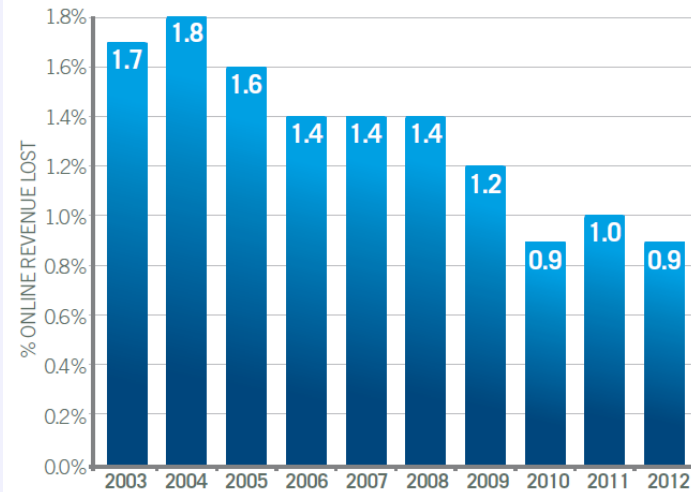
The Open Web Application Security Project

Why is Fraud Management important?

ESTIMATED REVENUE LOST DUE TO ONLINE FRAUD



AVERAGE FRAUD RATE BY REVENUE



(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.



OWASP

The Open Web Application Security Project

Not all thieves enter through your window!



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