

# Organized Fraud:

## What You Should Know About Chargebacks, Gold Farming & Account Takeovers

**Arthur Chu**

Fraud & Investigation Manager - Nexon America

**GAME DEVELOPERS CONFERENCE**

SAN FRANCISCO, CA  
MARCH 5-9, 2012  
EXPO DATES: MARCH 7-9

**2012**

# **Content Slide**

- **Gold Farming**
- **The Golden Triangle Of Fraud**
- **Mechanic Of Fraud**
- **How Credit Card Fraud Can Damage A Company**
- **Working With Publishers**
- **Evolution Of Gold Farmers & Sellers**
- **Account Takeover**
- **Trends in Account Takeover in Gaming**
- **Consumer Education is Important**
- **Are You Really Safe?**
- **Technology**
- **Some Account Takeover Detection**
- **Safe Practices**

# How We Normally Picture Gold Farmers



# The Darker Side Of Gold Farming & Selling



- Prisoners Were Used To Farm Gold Since 2004 And Possibly Earlier
- Cheap Labor – Free
- Huge Incentive To Succeed

"If I couldn't complete my work quota, they would punish me physically. They would make me stand with my hands raised in the air and after I returned to my dormitory they would beat me with plastic pipes. We kept playing until we could barely see things,"<sup>1</sup>

<sup>1</sup> <http://www.guardian.co.uk/world/2011/may/25/china-prisoners-internet-gaming-scam>

# Gold Selling Site

### Categories

**World of Warcraft US**

- >> Buy Gold
- >> Power Leveling
- >> Items
- >> Buy / Sell Account
- >> Instance

**World of Warcraft EU**

- >> Buy Gold
- >> Power Leveling
- >> Items
- >> Buy / Sell Account
- >> Instance

### Select Your Games

- World of Warcraft US
- Dragon nest
- Last Chaos
- World of Warcraft EU
- Dungeon Fighter Online
- Allods Online
- All Points Bulletin US
- All Points Bulletin EU
- land of chaos online
- Aika online
- knight online
- Runescape
- Final Fantasy XIV

**I Item List**   **II Shipping Info.**   **III Confirmation**

Choose Your Game / Server :

Game :

Server :

Oh, my old friend,  
Another Thanksgiving Day!  
Winter Solstice came and Thanksgiving Day is around the corner. We need real action to express the heart of Thanksgiving. We should feel gratitude to those people who love and care about us. We should put more effort to return the good life...  
There are so many things we should express our gratitude on this special day. But here I'd like to thank you totally because you are my friend. Thanks for your tolerance when I made something wrong to you; thanks for your help when I need you; thanks for your patience when I let you wait for a while; and thanks for everything you did, my friend.  
Warm thanksgiving wishes please contact our LIVECHAT service.  
Thank you very much!

G4P

### Your Account

Email:

Password:

[Signin](#)   [SignUp](#)

[Forgot Password?](#)

[My Browser Information.](#)

Need help? Please talk to our LiveChat.

**LIVECHAT**

Service email:  
gold4power@gmail.com

Telephone: 1-321-248-6873

**Notice:**

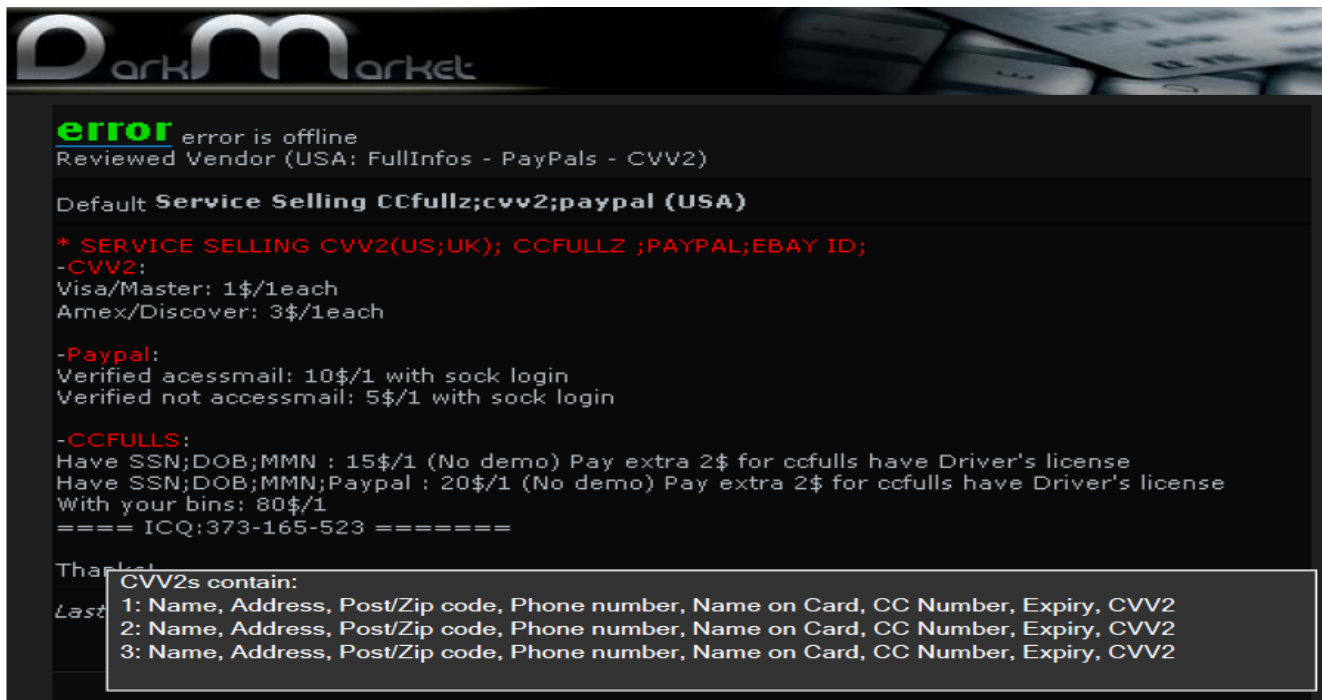
*Using illegal powerleveling/gold may suffer the risk of gaming account termination*

### contact us

Email:

- fig.dragon@gmail.com
- Yahoo: g4pcomplaint@yahoo.com
- Skype: mmopservice
- Tel: USA: +1 321 248 6873
- powerlevel

# Stolen Credit Cards Are Cheap



The image is a screenshot of a forum post on a website called 'DarkMarket'. The header of the forum shows the 'DarkMarket' logo and a background image of a keyboard and credit cards. The post itself is titled 'error is offline' and is a 'Reviewed Vendor' post. The vendor is selling stolen credit card information (CCFULLZ) and PayPal accounts (PAYPAL) for US dollars. The post lists prices for Visa/Master, Amex/Discover, and PayPal accounts, as well as the price for stolen credit card information (CCFULLZ) with various details like SSN, DOB, MMN, and Driver's license. The post also includes a contact ICQ number and a list of items contained in the CVV2s.

**error** error is offline  
Reviewed Vendor (USA: FullInfos - PayPals - CVV2)

Default **Service Selling CCFULLZ;cvv2;paypal (USA)**

**\* SERVICE SELLING CVV2(US;UK); CCFULLZ ;PAYPAL;EBAY ID;**  
**-CVV2:**  
Visa/Master: 1\$/1each  
Amex/Discover: 3\$/1each

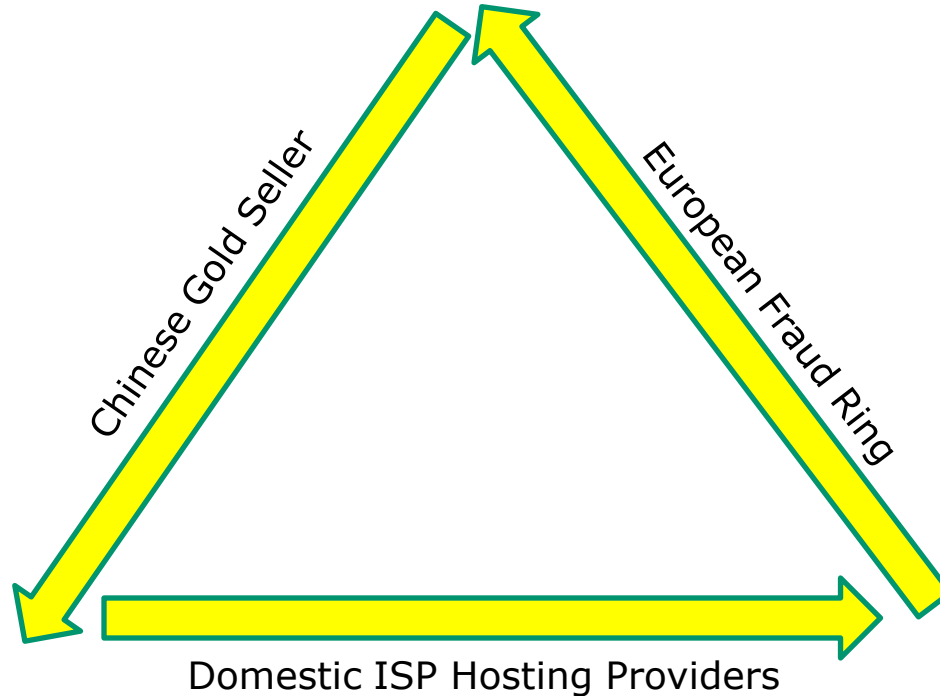
**-Paypal:**  
Verified accessmail: 10\$/1 with sock login  
Verified not accessmail: 5\$/1 with sock login

**-CCFULLS:**  
Have SSN;DOB;MMN : 15\$/1 (No demo) Pay extra 2\$ for ccfulls have Driver's license  
Have SSN;DOB;MMN;Paypal : 20\$/1 (No demo) Pay extra 2\$ for ccfulls have Driver's license  
With your bins: 80\$/1  
==== ICQ:373-165-523 =====

Thankst  
Last

**CVV2s contain:**  
1: Name, Address, Post/Zip code, Phone number, Name on Card, CC Number, Expiry, CVV2  
2: Name, Address, Post/Zip code, Phone number, Name on Card, CC Number, Expiry, CVV2  
3: Name, Address, Post/Zip code, Phone number, Name on Card, CC Number, Expiry, CVV2

# The Golden Triangle Of Gaming Fraud



# Their Roles In The Gaming Space

- European Fraud Rings
  - Steals Credit Cards Info
- Chinese Gold Sellers
  - Use Stolen Credit Cards
- Domestic ISP Hosting Providers
  - Services Them All

# Mechanics of Fraud

- If your game has any systems that place value on assets in the game AND makes them liquid, you are at risk
- Fraudsters need to be able to take or make assets and sell them
- Liquidity allows assets to take on a value
- Trade or Gifting

# How Can Credit Card Fraud Damage Company

## Business Case Study:

A Free 2 Play game company is evaluating the impact of chargebacks on their net profit. This company is a \$25 million dollar a year business with margins of 21.82% because they have an average rate of 5% chargeback a month and is considered a high risk merchant from the Visa/Mastercard association. Therefore, the chargeback fee increases to **\$100** per incident and also there is a set monthly fee imposed by Visa/MasterCard. What would happen if it increased further to 10% or reduced to 3%. I've also included what a sample of what the business profit margin would be if they had under 1% chargebacks and were not in the high risk program by Visa/Mastercard association.

# Chargeback At 5%

<b>Assumptions</b>				
Average Order Amount			\$	25
Orders				1,000,000
Chargeback Rate				5%
<b>Impact to Operations</b>				
Revenue			\$	25,000,000
Credit Card Transaction Fees	3.50%		\$	875,000
Bank Refund to Cardholder			\$	1,250,000
No. of Transactions Chargeback				50,000
*Per Item Visa CB Fee (54%@\$100)			\$	2,700,000
Average Fee \$10				
**Per Item MasterCard CB Fee (46%@\$100)			\$	2,300,000
Average Fee \$10				
6 Months Visa High-risk Fee (\$20K/Month)			\$	120,000
6 Months MasterCard High-risk Fee (\$50K/Month)			\$	300,000
<b>Total Impact of Chargeback and Fees</b>			\$	7,545,000
Revenue Net Chargeback				
Impact on Revenue				30.18%
Operating Expense per Order			\$	12.00
*Fraud Expense per Order			\$	7.55
<b>Margin</b>				21.82%

# Chargeback Impact To Revenue At 10%

<b>Assumptions</b>					
Average Order Amount			\$ 25	\$ 25	
Orders			1,000,000	1,000,000	
Chargeback Rate			5%	10%	
<b>Impact to Operations</b>					
Revenue			\$ 25,000,000	\$ 25,000,000	
Credit Card Transaction Fees		3.50%	\$ 875,000	\$ 875,000	
Bank Refund to Cardholder			\$ 1,250,000	\$ 2,500,000	
No. of Transactions Chargeback			50,000	100,000	
*Per Item Visa CB Fee (54%@\$100)			\$ 2,700,000	\$ 5,400,000	
Average Fee \$10					
**Per Item MasterCard CB Fee (46%@\$100)			\$ 2,300,000	\$ 4,600,000	
Average Fee \$10					
6 Months Visa High-risk Fee (\$20K/Month)			\$ 120,000	\$ 120,000	
6 Months MasterCard High-risk Fee (\$50K/Month)			\$ 300,000	\$ 300,000	
<b>Total Impact of Chargeback and Fees</b>			\$ 7,545,000	\$ 13,795,000	
Revenue Net Chargeback					
Impact on Revenue			30.18%	55.18%	
Operating Expense per Order			\$ 12.00	\$ 12.00	
*Fraud Expense per Order			\$ 7.55	\$ 13.80	
<b>Margin</b>			21.82%	-3.18%	

# Comparison When Reduced To 3%

<b>Assumptions</b>							
Average Order Amount				\$ 25	\$ 25	\$ 25	
Orders				1,000,000	1,000,000	1,000,000	
Chargeback Rate				3%	5%	10%	
<b>Impact to Operations</b>							
Revenue				\$ 25,000,000	\$ 25,000,000	\$ 25,000,000	
Credit Card Transaction Fees 3.50%				\$ 875,000	\$ 875,000	\$ 875,000	
Bank Refund to Cardholder				\$ 750,000	\$ 1,250,000	\$ 2,500,000	
No. of Transactions Chargeback				30,000	50,000	100,000	
*Per Item Visa CB Fee (54%@\$100)				\$ 1,620,000	\$ 2,700,000	\$ 5,400,000	
Average Fee \$10							
**Per Item MasterCard CB Fee (46%@\$100)				\$ 1,380,000	\$ 2,300,000	\$ 4,600,000	
Average Fee \$10							
6 Months Visa High-risk Fee (\$20K/Month)				\$ 120,000	\$ 120,000	\$ 120,000	
6 Months MasterCard High-risk Fee (\$50K/Month)				\$ 300,000	\$ 300,000	\$ 300,000	
<b>Total Impact of Chargeback and Fees</b>				<b>\$ 5,045,000</b>	<b>\$ 7,545,000</b>	<b>\$ 13,795,000</b>	
Revenue Net Chargeback							
Impact on Revenue				20.18%	30.18%	55.18%	
Operating Expense per Order				\$ 12.00	\$ 12.00	\$ 12.00	
*Fraud Expense per Order				\$ 5.05	\$ 7.55	\$ 13.80	
<b>Margin</b>				<b>31.82%</b>	<b>21.82%</b>	<b>-3.18%</b>	

# Under 1% Chargeback

## What Is The Difference In 2%?

Assumptions							
Average Order Amount		\$ 25		\$ 25		\$ 25	
Orders		1,000,000		1,000,000		1,000,000	
Chargeback Rate		0.99%		3%		5%	
Impact to Operations							
Revenue		\$ 25,000,000		\$ 25,000,000		\$ 25,000,000	
Credit Card Transaction Fees	3.50%	\$ 875,000		\$ 875,000		\$ 875,000	
Bank Refund to Cardholder		\$ 247,500		\$ 750,000		\$ 1,250,000	
No. of Transactions Chargeback		9,999		30,000		50,000	
*Per Item Visa CB Fee (54%@\$100)		\$ 53,995		\$ 1,620,000		\$ 2,700,000	
Average Fee \$10							
**Per Item MasterCard CB Fee (46%@\$100)		\$ 45,995		\$ 1,380,000		\$ 2,300,000	
Average Fee \$10							
6 Months Visa High-risk Fee (\$20K/Month)		0		\$ 120,000		\$ 120,000	
6 Months MasterCard High-risk Fee (\$50K/Month)		0		\$ 300,000		\$ 300,000	
Total Impact of Chargeback and Fees		\$ 1,222,490		\$ 5,045,000		\$ 7,545,000	
Revenue Net Chargeback							
Impact on Revenue		4.89%		20.18%		30.18%	
Operating Expense per Order		\$ 12.00		\$ 12.00		\$ 12.00	
*Fraud Expense per Order		\$ 1.22		\$ 5.05		\$ 7.55	
Margin		47.11%		31.82%		21.82%	

# Working with Publishers

## **I Work With A Publisher, They Handle All That Stuff. Why Should I Care About Chargeback?**

- Facebook, Apple, Steam, and MMO publishers like Nexon
- Or, my payments provider guarantees against chargeback
- If the game generates high fraud activity any company would shut you down from payments which means no money
- There are certain mechanic or item in a game you just cannot change but causes a lot of fraud
- Nexon uses a prepaid option to still monetize and take the chargeback risk out

# What Is Prepaid & How Does It Help?



# Gifting

## Cash Shop



## Evolution Of Gold Farmer & Seller

Gold Farming With Manual Labor



Gold Farming With Bots



Credit Card Fraud



Account Takeover

# Account Take-Over

Account takeover is one of the more prevalent forms of identity theft. It occurs when a fraudster obtains an individual's personal information (account number and social security number usually suffice), and changes the official mailing address with that individual's financial institution (FI). Once accomplished, the fraudster has established a window of opportunity in which transactions are conducted without the victim's knowledge.

Account takeover is becoming increasingly prominent and is a growing point of financial exposure for Financial Institutes, businesses, and consumers. Reducing exposure is best accomplished through a combined approach of Process, Consumer Education, and Technology.

## **Fraud Alert Involving Unauthorized Wire Transfers To China 26 April 2011**

The FBI has observed a trend in which cyber criminals — using the compromised online banking credentials of U.S. businesses — sent unauthorized wire transfers to Chinese economic and trade companies located near the Russian border. Between March 2010 and April 2011, the FBI identified twenty incidents in which the online banking credentials of small-to-medium sized U.S. businesses were compromised and used to initiate wire transfers to Chinese economic and trade companies. As of April 2011, the total attempted fraud amounts to approximately \$20 million; the actual victim losses are \$11 million.

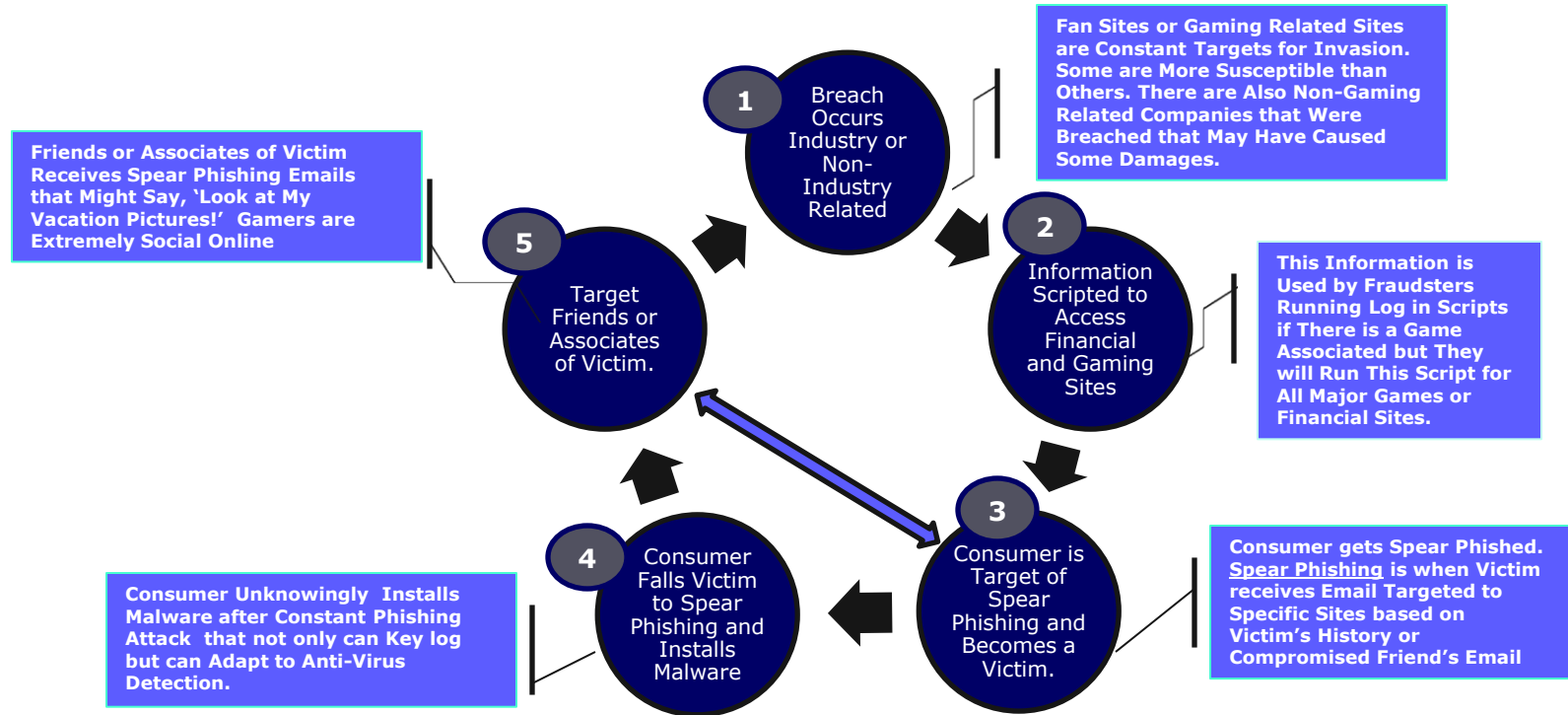
[http://www.bankersonline.com/vendor\\_guru/pps/pps\\_takeover.html](http://www.bankersonline.com/vendor_guru/pps/pps_takeover.html)

<http://www.ic3.gov/media/2011/ChinaWireTransferFraudAlert.pdf> Internet Crimes Complaint Center

# Financial Related Attack Dissected By FBI & FSIAC



# Recent Trend Of Account Take Over In Gaming



# Consumer Education Is Important

- Companies Will Never Ask For Password – **They Have It!**
- Do Not Respond To Or Open Attachments Or Click On Links In E-mails.
- Be Careful Of Free Apps Or Games For Smart Phones. Smartphone Users Were About A Third More Likely To Become Victims Than Non-users (Based On Javelin Strategy & Research)
- Do Not Post Private Information (Birthdates Or At Least Omit Year of Birth, Home Address, Ect) On Public Social Sites
- Be Wary Of Pop-up Messages Claiming Your Machine Is Infected And Offering Software To Scan And Fix The Problem, As It Could Actually Be Malicious Software That Allows The Fraudster To Remotely Access And Control Your Computer.
- Do Not Use Public Internet Access Points (e.g., Internet Cafes, Public Wi-Fi Hotspots (Airports, Etc.) To Access Accounts Or Personal Information. If Using Such An Access Point, Employ A Virtual Private Network (VPN)

# Consumer Education Part II

- Keep Operating Systems, Browsers, And All Other Software & Hardware Up-to-date.
- Keep Up-to-date Of The Continuous Cyber Threats That Occur.
- As Recommended By Microsoft For Users More Concerned About Security, Many Variants Of Malware Can Be Defeated By Using Simple Configuration Settings Like Enabling Microsoft Windows XP, Vista, And 7 Data Execution Prevention (DEP) And Disabling Auto Run Commands.
- Identity Theft Sometimes Often Happens From People You Know
- Phishing E-Mails Have Become More Sophisticated -> Spear Phishing
- Your Identity And Some Personal Information Is Probably Already Out There
- Research firm Javelin Strategy & Research Found Someone Whose Personal Information Is Taken In A Data Breach Is 9.5 Times More Likely To Become a Victim of Identity Fraud. **Heyyyy...That's Me!**

# Are You Really Safe?



**LifeLock**  
Guarantee Your Good Name

LifeLock for People | LifeLock for Business | Our Guarantee | About Us | Enroll Now ▶ | 1 877 LI

**My name is Todd Davis**  
**This is my social security number 457-55-5462**

"I'm Todd Davis, CEO of LifeLock. Yes, that really is my social security number. No I'm not crazy. I'm just sure our system works. Just like we have with mine, LifeLock will make your personal information useless to a criminal. And it's **GUARANTEED.**"

Here at LifeLock, We Guarantee Your Good Name.  
No one else does because no one else can.

**More Testimonials:**  
Stop Junk Mail. Stop Credit Offers.  
Stop Identity Theft. **Guaranteed.**

Enroll Now ▶

- He's been a [victim of identity theft at least 13 times](#), according to the *Phoenix New Times*.
- That's 12 more times than has previously been known.
- In June 2007, Threat Level reported that Davis had been the victim of identity theft after someone [used his identity to obtain a \\$500 loan](#) from a check-cashing company.<sup>2</sup>
- Moral of the story, do not post sensitive personal information in public media

<sup>2</sup> <http://www.wired.com/threatlevel/2010/05/lifelock-identity-theft/>

# Technology That Are Available

- Being Able to Identify Your Customers is Key!
  - **Email Verification & Secret Questions - Out of Wallet Questions (Free)**  
Adds A Limited Barrier for Fraudsters To Take Over Accounts But If The Customer Information Is Already Compromised Then There Is Very Little Barrier For The Fraudsters.
  - **Geo-location Technology (Cheap and Affordable)**  
Geo-location Will Identify IP, ISP/Hosting Providers, City & State Of Users  
Combination Of Geo-location, Secret Questions, Email Verification & Cookies Can Provide Some Measure Of Identifier But Can Cause Heavy Friction To Users If Implemented Incorrectly Which Will Be Somewhat Limited In Effectiveness.
  - **Account + Device Picture Association Or Sitekey**  
Picture Is Better At Explaining This.



Your SiteKey®:

goyangi



If you don't recognize your personalized SiteKey®, don't enter your Passcode.

\* Passcode:

(8 - 20 Characters, case sensitive)

# Technology Part II

- **Device Fingerprinting Technology**

Identifies Unique Devices Mobile Or Computer

Combination Of Geo-location And Device Technology Can Make A Very Useful Customer Identifier But Can Be Cost Based on Volume.

- **SMS (Short Message Service)**

This Service Can Be Used For Verification Or If Customer Triggers Certain Flags That Can Normally Deny Access Or Transactions But Can Use This For Verification To Access. Also Has A Cost Association With Volume.

- **OTP (One Time Password)**

Mobile Or Physical Device That Delivers A Single Use Password For Every Instance of Login Or Transaction Depending On Business. There Is A Cost To This Technology And Should Always Be Optional For Users As It Would Create An Extreme Barrier and Friction If Forced. Often Times Heavy Incentive Is Given to Users To Subscribe

# **What Do All These Solutions Have In Common?**

## **Major Banks Uses All Of Them!**

Which Means Fraudsters Have Had A LOT Of Practice  
at Compromising Accounts.

# Some Account Take-Over Detection Methods

- **Once You Can Identify Your Customer, There Are A Few Method Of Detection**

- Change To Registered Email
- Change Or Adding New Credit Card
- Change In IP
- Change In Behavior Based On Customer History
- Changed Password
- Known List Of Bad IP (ISP/Hosting Providers & Proxys) That Have Logged Into An Account

**If Any Of The 2 Changes Are Made With-in A Very Short Time Period Then The Account Should Be Flagged For Review.**

# More Safe Practices

- **Analyze Logs to Determine Trends of Take-Over Accounts (Post Analysis)**  
Understand Your Game & The Economy. Most Of The Fraud Takes Place In The Games  
Create A Review System Or Team To Spot Trends  
Build & Design Logs For Things That Happen In Game  
If Possible, Create Fraud Rule System That Can Changed Rule Settings (Thresholds) On The Fly
- **Built or Design Some Barriers Of Entry To Reduce Take-Over**  
Some Friction For Registration Is Almost Required For This Time & Age- Captcha Does Not Cut It  
You Can Use The Technology Discussed To Create Some Minimal Challenges That Will Identify Users
- **Give Incentive to Consumers to Change Passwords**  
Maybe Doing Quarterly Or Bi-Annual Incentives For Users To Change Password by Possibly Giving In-Game Incentives.  
Make Sure The Password Changed Cannot Be The Same One In The User's History
- **Never Underestimate The Farmer Just Because They Are Called Farmers**  
If One Out of One Thousand Is Born a Genius, We Are Way Outnumbered. Almost 5 To 1 If The Population Census Is Rounded Up. That Is Just For One Specific Country Doing Fraud.

# Q & A

