# Best Practices to Prevent Internet Fraud

Presented by:
Ori Eisen
Founder & Chief Innovation Officer

# Start with a laugh…

P.C. Vey, Published by the New Yorker, January 16th, 2006

# The Art of War – Know Your Enemy

If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle.

- Sun Tzu On the Art of War, about 530 BCE

# Let's Play Tag

- Pros and Cons of Different CDIs
  - Tag (Flash, Cache, Cookie, etc.)
  - Tag-less (HTTP headers, Java script, etc.)
- IP Address is NOT a CDI!!!
  - Much like your clothes are not part of your DNA

# Tag You're Not It

- VMWare
- Disable Cookies
- Uninstall Flash
- Mobile Devices Do Not Support Flash
- Anti-virus and anti-Malware delete tags regularly
- 100% Right or 100% Wrong
- Good for detecting good people
- Not good for detecting the medium to highly sophisticated fraudsters

# Fraud Is NOT a Game of Tag

## No problem

- VMWare
- Disable Cookies
- Uninstall Flash
- Anti-Virus and anti-malware delete tags regularly
- Mobile devices do not support

## Benefits

- 100% right or 100% wrong – more right than wrong
- Good for detecting good people…AND detecting ALL levels of medium to high sophistication of fraudsters

# Apple Pilot

## Analysis Strategy

- Determine how Device ID can augment current fraud systems
- Analysis to focus on detecting more fraud $

1. Record Device Ids for all fraud orders for first 20 days of pilot
2. Match ids against orders in last 10 days
3. Measure following metrics
   - Total fraud $ matched per day
   - Total unblocked $ matched per day
   - % of total fraud $ covered
   - Total orders covered per day
   - False positive rate

# Results

| | PC Print | Cache ID | Cookie ID |
|---|---|---|---|
| % of total fraud covered | 19.5% | 0.14% | 1.7% |
| % unblocked fraud covered | 30.4% | 0.0% | 0.2% |
| False positive rate | 45.2% | 62.5% | 40.7% |

# A Customer's View

"From that analysis [of the pilot], my conclusion is that tagging is useful for recognizing good guys, but not for stopping fraud. The good fraudsters defeat the tags. The ones that don't are easily caught through more basic tools (e.g., AVS, CVV2, velocities, etc.)."

*David Moriarty, Ph.D.,*

*Apple, Inc.*

# What Others Say About Us?


"A solution that looks beyond HTTP parameters to fingerprint a PC… is now only available from The 41st Parameter.

We recommend this option as the strongest clientless CDI option available on the market today."

- After The Cookies Crumble: Alternatives for Client Device Identification (17 February 2007)

# The First 40 Parameters

## Is This Fraud?

**Order Information and Web Logs**

| A | B | C | D | E | F |
|---|---|---|---|---|---|
| Order ID | Order Timestamp | Billing Email | Billing Zip Code | Browser IP | Browser IP Country |
| 1358955 | 10/13/11 12:17 AM | vinhnguyen509@hotmail.com | 99202-4011 | 67.185.8.115 | United States |
| 1392535 | 10/13/11 3:52 AM | sandrita_1017@hotmail.com | 94559 | 76.103.150.225 | United States |
| 2396715 | 10/13/11 4:38 AM | yeaokwhatever05@hotmail.com | 92703-2632 | 75.31.69.233 | United States |
| 3672519 | 10/14/11 1:30 PM | timjiles@yahoo.com | 53209 | 76.199.175.61 | United States |
| 5921199 | 10/16/11 4:31 PM | mattaliano_electric@yahoo.com | 95037 | 71.80.231.193 | United States |
| 5879575 | 10/16/11 5:20 PM | bigkidjj@yahoo.com | 95355-7891 | 76.20.120.67 | United States |
| 5970599 | 10/16/11 9:15 PM | lsutton@lynndaleinc.org | 30805-3617 | 69.254.8.233 | United States |
| 7297735 | 10/18/11 3:29 PM | pinder_k05@yahoo.com | 94587 | 75.6.231.37 | United States |
| 7410155 | 10/19/11 12:43 AM | cmwhitson@prodigy.net | 21158-4219 | 71.125.171.155 | United States |
| 9729255 | 10/20/11 7:34 PM | jorgedc006@yahoo.com | 94062 | 69.104.90.240 | United States |
| 9753095 | 10/20/11 9:19 PM | kmlbnz@yahoo.com | 33142 | 76.26.50.51 | United States |
| 9774515 | 10/20/11 11:03 PM | newcenturymedsup@yahoo.com | 91205 | 68.183.218.68 | United States |

# How About Now?

| H | I | J | K | L |
|---|---|---|---|---|
| Browser Timestamp | Browser Time Zone | Browser Language | PCPrint | Time Diff (TDL) Seconds |
| 10/11/07 5:17 PM | 3 | ru-ru | 7B02A8AC99067CC1168E412B6AA0BF138E76CD84 | -3601 |
| 10/11/07 8:52 PM | 3 | ru-ru | 7B02A8AC99067CC1168E412B6AA0BF138E76CD84 | -3601 |
| 10/11/07 9:38 PM | 3 | ru-ru | 7B02A8AC99067CC1168E412B6AA0BF138E76CD84 | -3601 |
| 10/13/07 6:30 AM | 3 | ru-ru | 7B02A8AC99067CC1168E412B6AA0BF138E76CD84 | -3601 |
| 10/15/07 9:31 AM | 3 | ru-ru | 7B02A8AC99067CC1168E412B6AA0BF138E76CD84 | -3601 |
| 10/15/07 10:20 AM | 3 | ru-ru | 7B02A8AC99067CC1168E412B6AA0BF138E76CD84 | -3601 |
| 10/15/07 2:15 PM | 3 | ru-ru | 7B02A8AC99067CC1168E412B6AA0BF138E76CD84 | -3601 |
| 10/17/07 8:29 AM | 3 | ru-ru | 7B02A8AC99067CC1168E412B6AA0BF138E76CD84 | -3601 |
| 10/17/07 5:43 PM | 3 | ru-ru | 7B02A8AC99067CC1168E412B6AA0BF138E76CD84 | -3601 |
| 10/19/07 12:33 PM | 3 | ru-ru | 7B02A8AC99067CC1168E412B6AA0BF138E76CD84 | -3601 |
| 10/19/07 2:19 PM | 3 | ru-ru | 7B02A8AC99067CC1168E412B6AA0BF138E76CD84 | -3601 |
| 10/19/07 4:03 PM | 3 | ru-ru | 7B02A8AC99067CC1168E412B6AA0BF138E76CD84 | -3601 |