Stolen Data Markets: An Economic and Organizational Assessment

Thomas J. Holt
Michigan State University
holtt@msu.edu

Olga Smirnova
Eastern Carolina University

Yi-Ting Chua
Michigan State University

This project was supported by Award No. 2010-IJ-CX-1676, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not reflect those of the Department of Justice.

Stolen Data Markets

- There is an increasingly large body of research on the organization and dynamics of the market for stolen data
  - IRC (Franklin et al., 2007; Herley & Florencio, 2010; Holz et al., 2009; Honeynet Research Alliance, 2003; Thomas & Martin, 2006)
  - Forums (Chu et al., 2010; Holt & Lampke, 2010; Motoyama et al., 2011; Yip et al., 2013)

Stolen Data Markets

- Few studies have estimated the economics of the market or the organizational dynamics present

- Herley and Florencio (2010) and Wehinger (2011) argue that there may be multiple markets operating at any point in time
  - Lower priced markets with greater risk for participants and minimal barriers to entry
  - Higher priced markets with insularity, trust, and organization

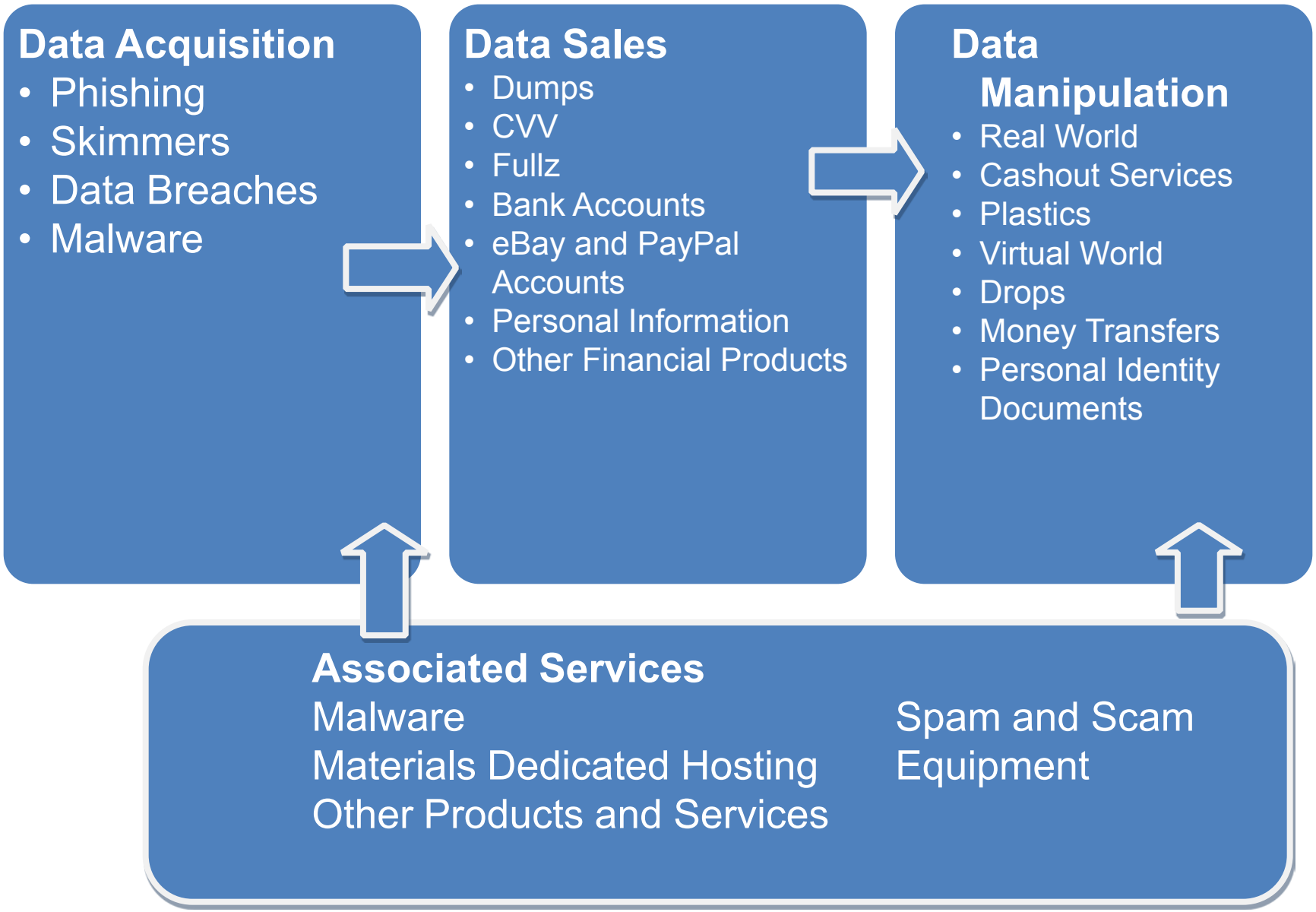
The Present Study

- This study is designed to address multiple questions:
  - What are the costs for goods and services in this market like and what conditions impact this economy?
  - What is the social organization of the market and how does it affect participants?
  - What are the network structures between individual participants and how do they resemble other criminal organizations?

Data Sources: 13 Active Forums

Forum	Descriptive Statistics for Forums Sampled (n=13)		
	Number of Threads	***Hosting Country***	***Language***
1	55	DE	RU
2	128	US	ENG
3	6	US	RU
4	144	VG	RU
5	89	UK	RU
6	44	RU	RU
7	202	RU	ENG/RU
8	590	LV	ENG
9	312	RU	ENG/RU
10	35	DE	RU
11	60	RU	RU
12	71	NL	RU
13	153	LU	RU

Economic Analyses- Products Sold

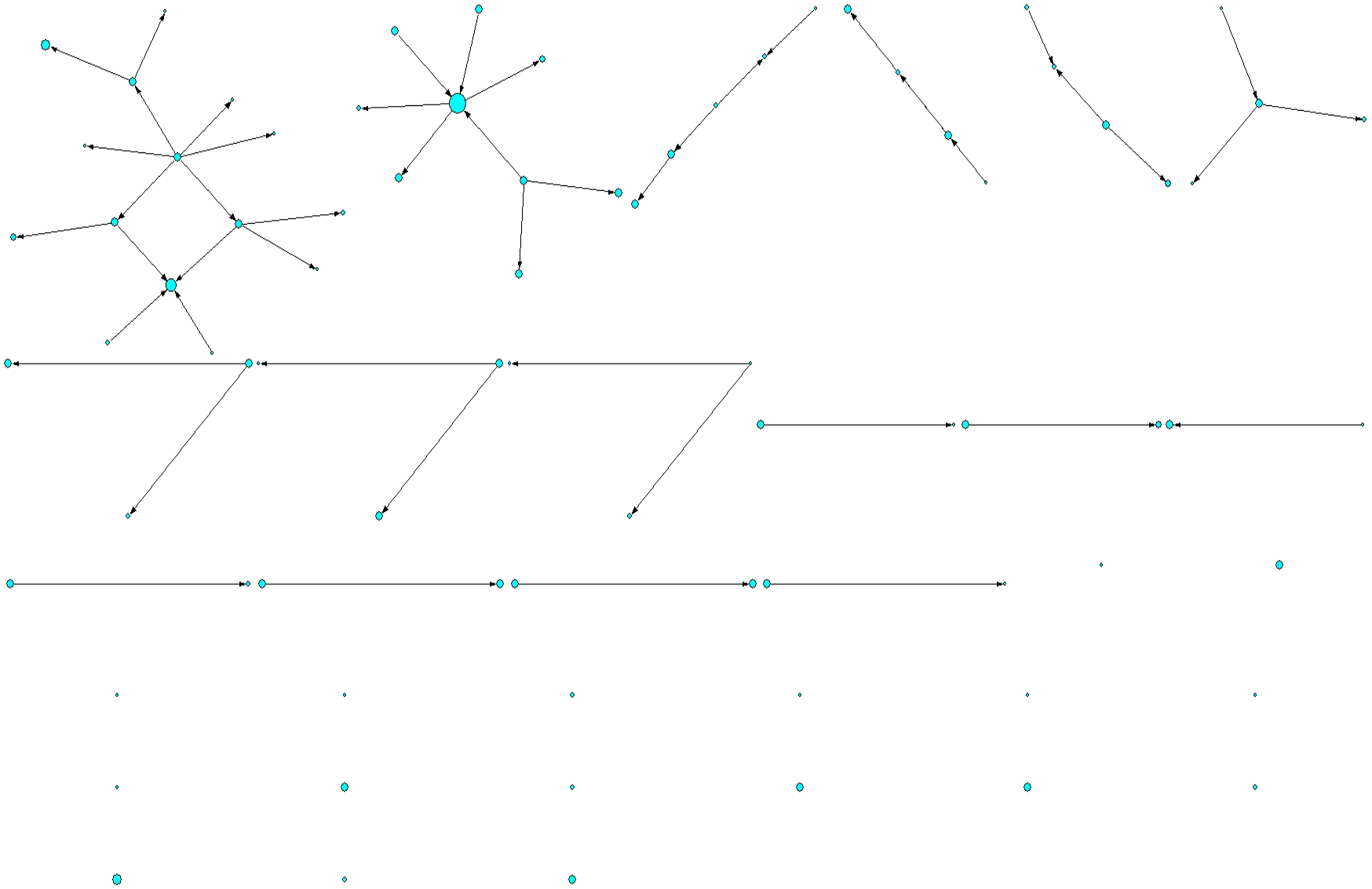


Organizational Analyses

- This study utilizes the framework of organizational sophistication developed by Best and Luckenbill (1994)

Forms of Organization	Characteristics	.		
	Mutual Association	Mutual Participation	Division of Labor	Extended Duration
Loners	No	No	No	No
Colleagues	Yes	No	No	No
Peers	Yes	Yes	No	No
Teams	Yes	Yes	Yes	No
Formal Organizations	Yes	Yes	Yes	Yes

Social Network Analyses



The Markets and Their Operations

The Sales Process

- The sales process involves mutual association and participation

Seller Posts an Ad in Forum

Dumps Fresh Base ... EU-USA-CANADA-ASIA-OTHER.. Best Valid..
PRICE LIST:
**********USA**********
1pcs CLASSIC/STANDARD= 20$
1pcs GOLD/PLATINUM = 25$
1pcs BUSINESS/SIGNATURE/PURCHASE/CORPORATE/WORLD = 30$
1pcs AMEX = 20$
**********CANADA**********
1pcs CLASSIC/STANDARD = 50$
1pcs GOLD/PLATINUM/BUSINESS/SIGNATURE/PURCHASE/CORPORATE/WORLD = 70-200$
*******EUROPE & ASIA & LATIN & OTHERS*********
---[code 101 - non chip]---
1pcs CLASSIC/STANDART = 110$
1pcs GOLD/PLATINUM = 130$
1pcs BUSINESS/SIGNATURE/PURCHASE/CORPORATE/WORLD = 150$
1pcs INFINITE = 200$
****

The Sales Process

- The sales process involves mutual association and participation

Seller Posts an Ad in Forum

RULES:
(please read the rules carefully and follow all the steps, anyone breaking this rules shall expect to be fully ignored by service)
1. Contact with one of the our supports and choose dumps u want.
2. Calculate total price and submit your order.
3. Send us money and your e-mail.
4. We have 24 hours (maximum) to complete your order.(LR [Liberty Reserve Payment] INSTANT DELIEVERY)
5. We replace only Pickup/Hold Call Dumps with in 24 hours after time period we are not responsible
PAYMENT INFO:
LIBERTY RESERVE
Support Icq: [removed]

The Sales Process

- The sales process involves mutual association and participation

Seller Posts an Ad in Forum

- Let us introduce ourselves: we are the trusted sellers of the PayPal accounts.
  You'll find lots of **USA/UK**:
  Unverified + Credit Cards (confirmed) → 1 WMZ/LR
  Unverified + Bank Acc (confirmed) → 1 WMZ/LR
  Verified + Credit Cards (confirmed) + Bank accounts (confirmed) → 3 WMZ/LR
- We also have **accounts with email**-just ask and we'll let you know.
  We accept both: **Webmoney / Liberty Reserve**
  Here are some rules of the service:
- => Seller is not responsible for SM (security measures); we check all the accounts manually prior giving them to you. You'll also get a clean socks5.
  => Seller is not reponsible for the unsuccessfull usage of the account.

The Sales Process

- The sales process involves mutual association and participation

Seller Posts an Ad in Forum

We are the experience team [name removed] working in the area of banking innovations, and here on the site we are ready to offer you the following services:
We in cash funds in the RF [Russian Federation] which we have received as electronic bank transfers.
Help with encashment: direct scheme- no intermediaries
-encashment of funds
-Transmit of electronic funds
-Diversion of funds
-Work with accounts that have been seized by the authorities
Work with dirty funds
Our advantages:
-Low commissions
-Speed (as a rule, funds are received on the day that they are credited to our company's account (usually on the day following the payment day in the RF), on the next day or maximum one day after crediting to our account depending on the amount.

Pricing Information for Products Sold

Product	Min Price	Max Price	Average Price	Count w/Price	%
Bank Accounts	5.00	700.00	187.44	63	30.7
Cashout Services	0.30	6000.00	1076.93	14	6.0
CVV	1.00	8000.00	26.21	4316	96.3
Dedicated Servers	0.20	700.00	100.97	42	26.7
Drops for Laundering	0.50	1000.00	192.37	27	16.4
Dumps	0.04	8000.00	102.60	5167	90.1
eBay/PayPal	0.20	800.00	27.25	118	64.4
Equipment	3.00	5000.00	549.51	61	30.8
Fullz	15.00	150.00	72.81	87	71.3
Identity Docs	0.50	500.00	138.46	32	40.0
Malware	2.00	1570.00	83.27	99	54.1
Money Transfers	10.00	38000.00	1424.59	37	52.2
Personal Info and Accounts	1.00	5025.00	197.19	44	44.4
Plastics	0.50	3000.00	261.47	47	30.7
Skimmers	200.00	9000.00	2382.60	23	18.4
Spam and Scams	8.00	600.00	96.33	24	16.4

Products Sold

- There is some variation in products based on the legitimacy of seller behavior

Including All Forums

1.	Dumps	5735
2.	CVV	4481
3.	Money Xfer	303
4.	Other Products	277
5.	Cashout Services	235
6.	Bank Accounts	205
7.	Equipment	198
8.	Malware	183
9.	Drops	165
10.	Dedicated Hosting	157

Excluding Two Forums

1.	Dumps	2748
2.	Cashout Services	196
3.	Other Products	170
4.	Malware	151
5.	Dedicated Hosting	139
6.	Drops	136
7.	Money Xfer	127
8.	eBay and Paypal	108
9.	Spam/Scam Materials	104
10.	Plastics	86

Price By Country

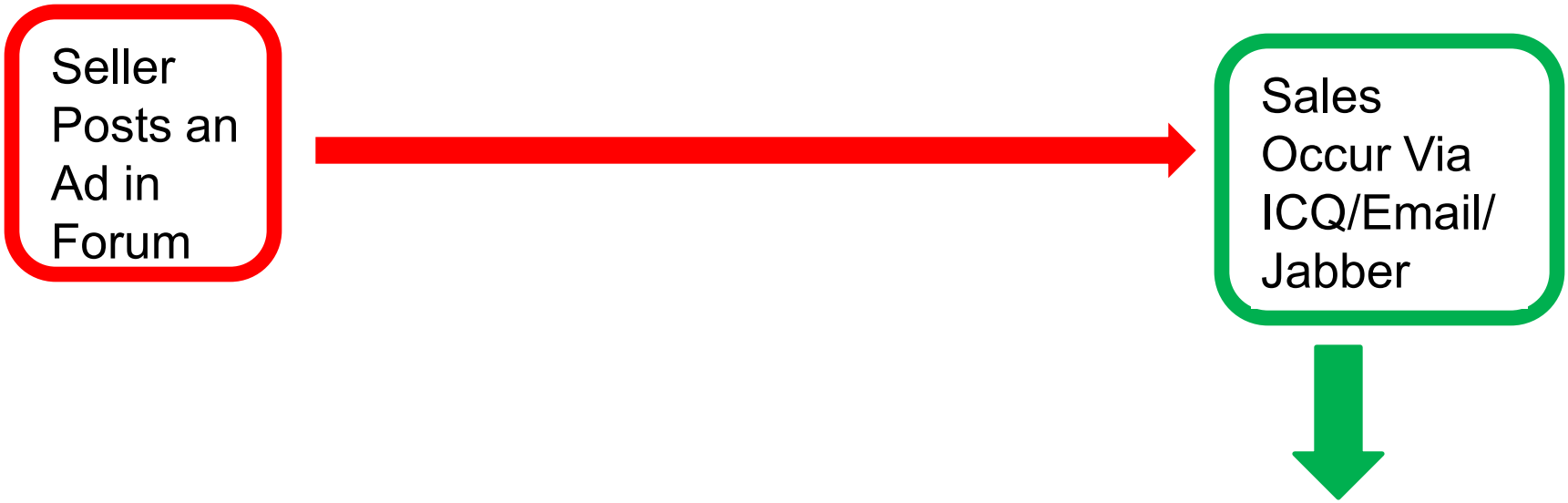
	Bank Accounts			Dumps		
	0	1	T	0	1	T
Asia	4.82	4.48	0.54	3.57	4.32	-12.31***
Australia and New Zealand	0	0	0	3.64	3.29	3.21***
Canada	4.74	5.25	-1.06	3.67	3.37	5.90***
Europe	4.95	4.12	2.22*	3.49	4.02	-14.17***
Other	4.76	5.09	-0.63	3.52	4.48	-19.09***
Russia	0	0	0	3.64	3.85	-0.50
United Kingdom	4.82	4.08	0.85	3.69	2.81	13.00***
United States	4.68	5.33	-1.37	3.85	3.04	22.05***

* p≤.05 **p≤.01 ***p≤.001; 0= all other nations, 1= selected country

Notes: The binary measures were computed for each geographic category. That is, Bank Accounts sold in Asia (1) compared to all other accounts (0), and the T indicates the t-test measure.

Sales Process and Social Organization

- The sales process involves mutual association and participation



- Buyers place orders and pay for services electronically
  - Liberty Reserve, WebMoney (WM)
  - Western Union/MoneyGram
  - Escrow payments incorporating other forum users

Sales Process Facilitators

- Guarantor services

  The guarantor of a forum has been created so that you will not be deceived… By conducting a transaction through a guarantor, you can be sure that you will not be deceived.

- Terms for working through a guarantor:

  1. The buyer and the seller must reach agreement on working through a Guarantor.

  2. The buyer and the seller must contact the Guarantor using icq.

  3. One of the Parties to the transaction gives money to the Guarantor, and the other goods.

  4. The guarantor's services are free up to $30.

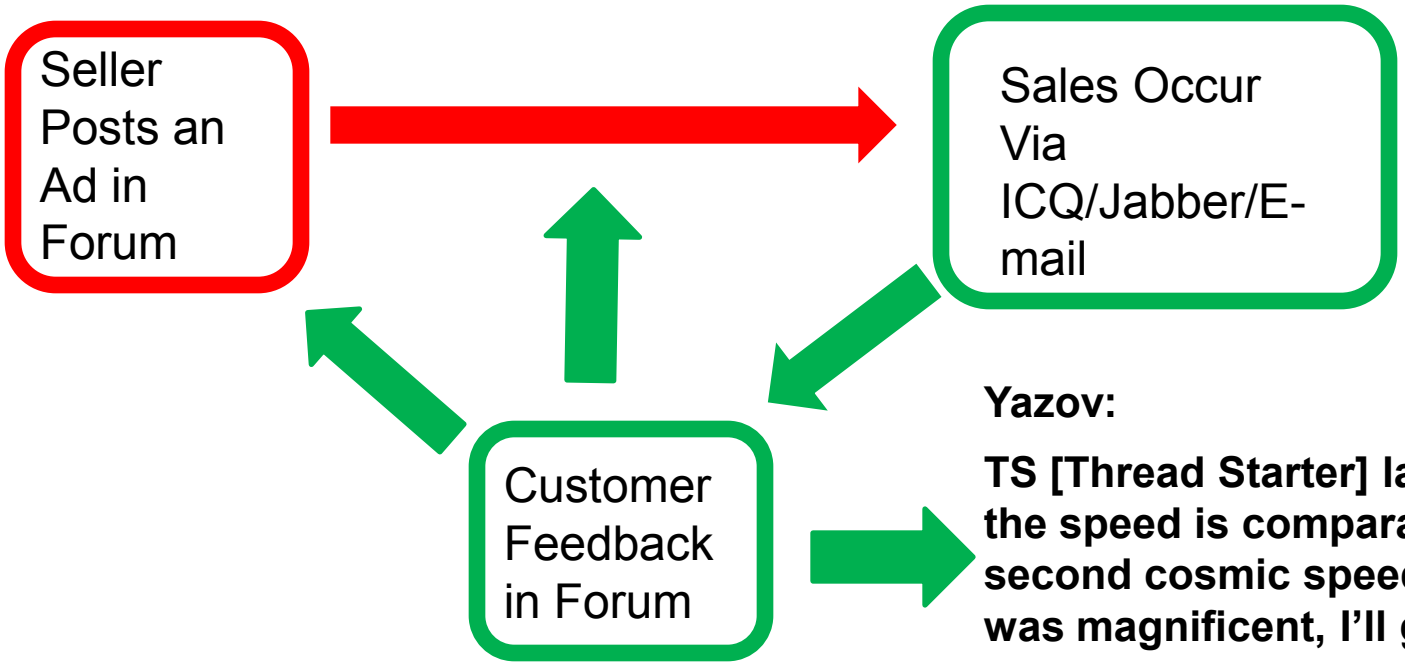
  up to 500 wmz - 8%

  from 500 wmz - 6%

  from 3000 wmz - 5%

Sales Process and Social Organization

- The sales process involves mutual association and participation



Yazov:

TS [Thread Starter] laundered $300, the speed is comparable to the second cosmic speed. Everything was magnificent, I'll go back

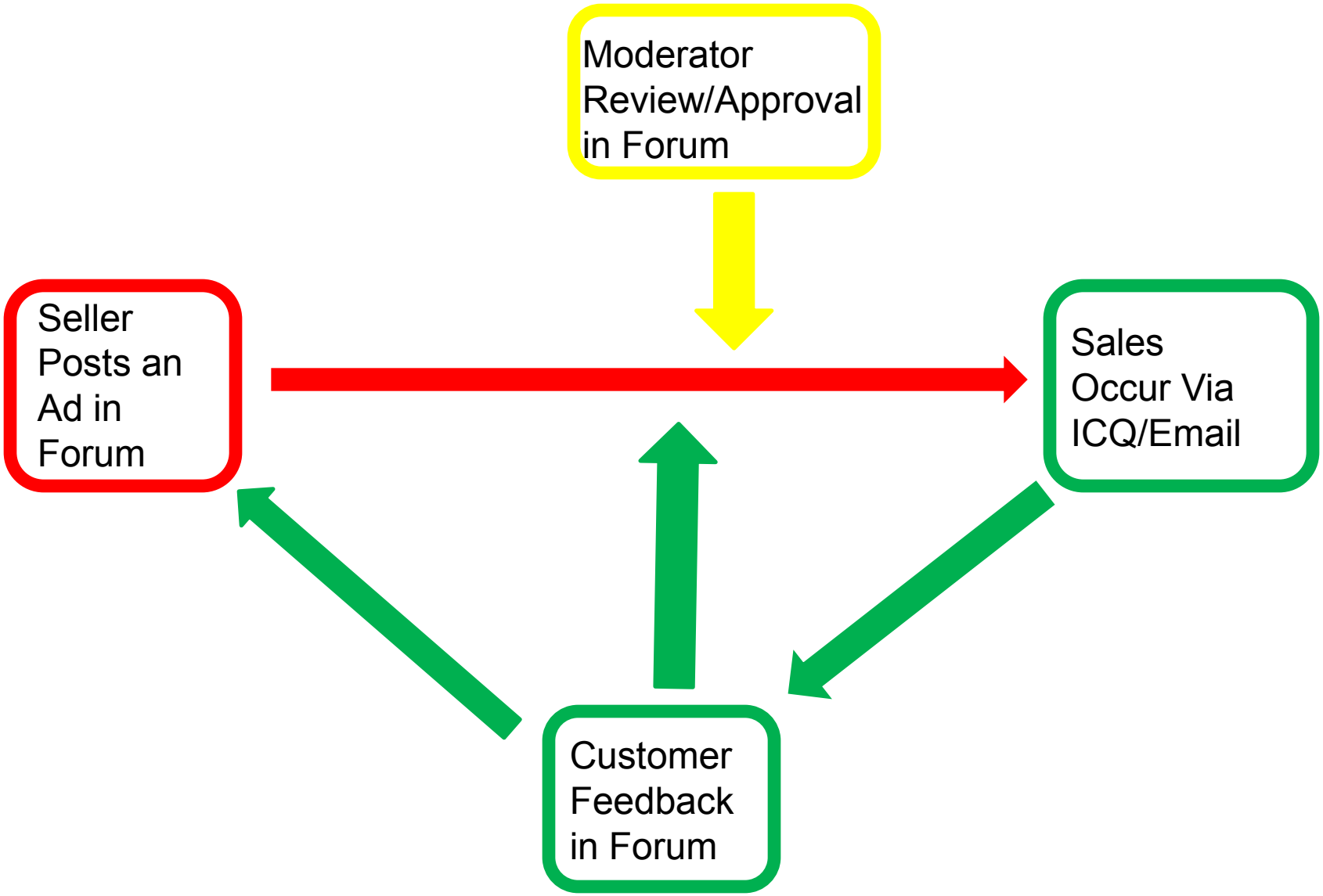
Avatar:

I did some laundering of money from a female partner, everything was quick and excellent and he [the TS] takes a small percentage, which also makes one happy.

Social Organization: Product Reviews

- Hans
  - Has your service been tested or vouched?
    I can provide potential business for you in the way of carding items…
- Bitmore
  - he is a **ripper**!!!don't believe him!his drops from florida
- Dentmer
  - I am no ripper, I have never had a complaint. This poster just wants to cause trouble. I have never dealt with him before. As you can see, there are no logs to back up his claim. Moderator please ban him.
- Kimpo
  - I have contacted with him on other forum!!!
    I asked him he accepts to pay escrow for guarantee.. Of course he refused!

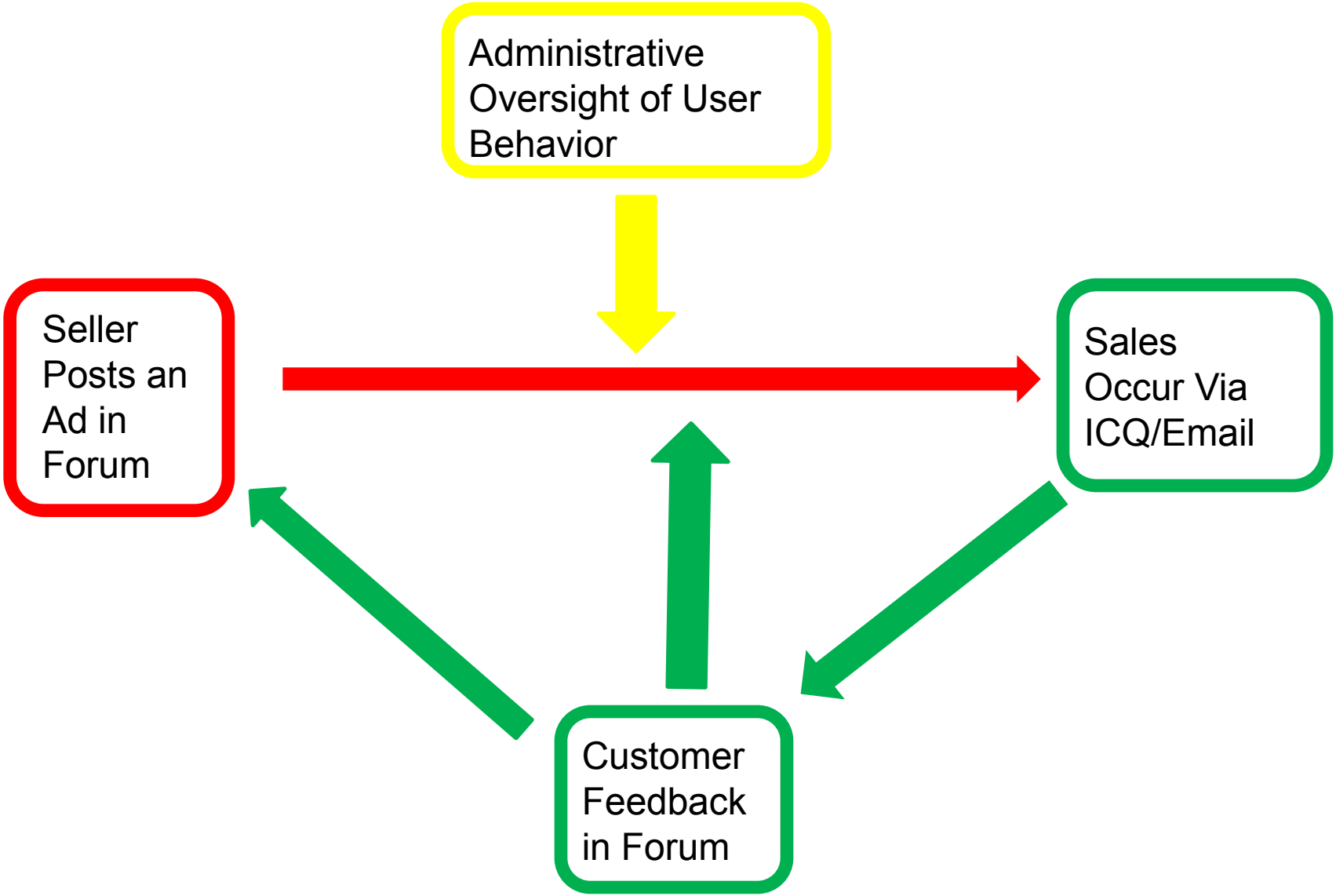
Sales Process and Social Organization



Social Organization: Product Testing

- **Checking Rules**
  Checking your goods will take place voluntarily or if the administration of the forum requires it.
  Checking of goods is done by **[name removed]**
  The check last from one to three days.
  After the check, the moderator guarantees that there will not be any stupid flames in the topic and that the quality of the goods will not be discussed. The moderator will write a review on this and close the topic. If a requirement to provide your product for testing is refused, you risk being banned, and your announcement will be erased. No money is taken for testing.
  You provide the product for the test in the same configuration in which you sell it

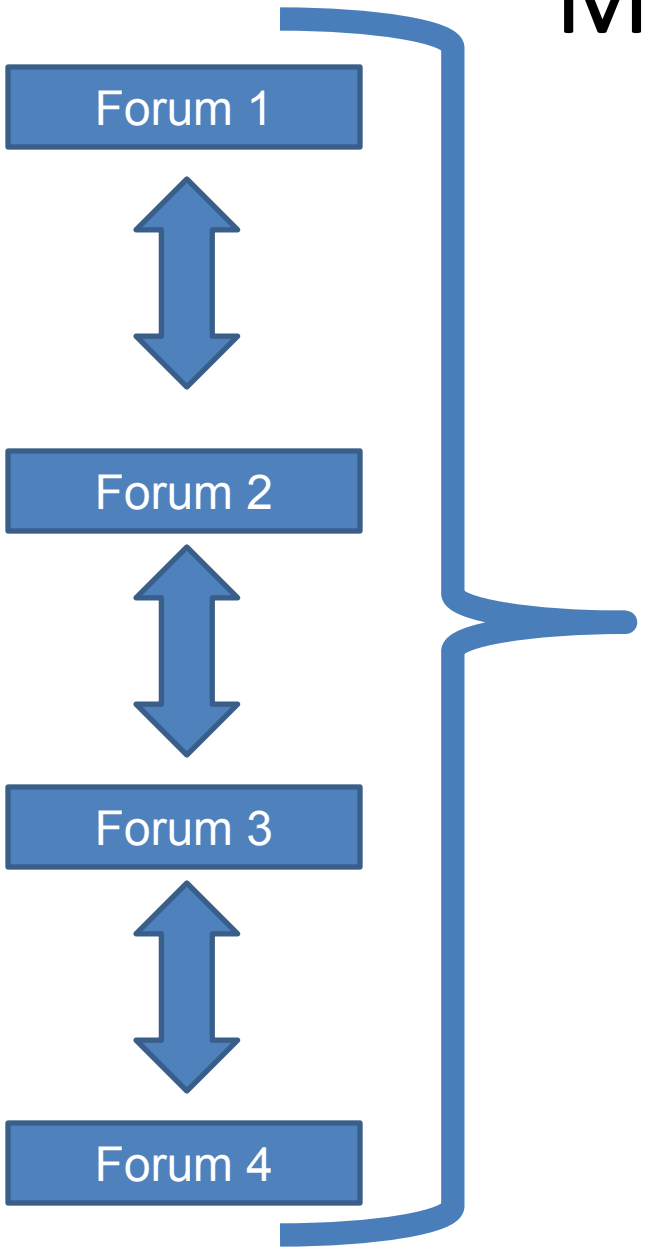
Social Organization of Markets



Forum Administration

- Forum Admins and Moderators can also manage the activities of users through bans
  - To leave fictitious rules in topics. The fact that a transaction has been carried out must be confirmed by the appropriate proof upon the first request of the administration. If this cause is violated, the user leaving a fictitious review will be banned, and perhaps even permanently..
  - To leave the following type of message: “TS [Thread Starter] is a burner [rip off artist] you shouldn’t have anything to do with him.” We will immediately post the logs proving guilt..
  - Reviews from users with 1-10 messages who have not been on the forum for long will be deleted at the discretion of the moderator.

Macro-Level Organization



When viewed in the aggregate, some of these forums act as formal organizations:

- Place to sell and buy
- Managerial structure
- Connections between forums
- Duration over time

The Economic Impact of Stolen Data Markets

Estimates of Seller Profits

Product	Non-Ripping	Ripping	Total
Bank Accounts	3	18	21
CVV	2	61	63
Dumps	190	67	257
Ebay/PayPal	6	3	9
Fullz	0	3	3
Total	201	152	353

Estimates of Seller Profits

- Data sellers have massive potential for profit
  - Using the average cost for data:
    - CVV=$26.21; 50 accounts=$1,310
    - Dumps= $102.60; 100 dumps= $10,260
    - ebay/PayPal= $27.25; 50= $1,362.50
  - Total transactions based on feedback
    - CVV= $82,561.50
    - Dumps= $2,636,820
    - eBay/PayPal= $11,938.50

Estimates of Buyer Profits

Product	Non-Ripping	Ripping	Total
Bank Accounts	1	12	13
CVV	0	25	25
Dumps	117	24	141
Ebay/PayPal	1	1	2
Fullz	0	1	1
Total	119	63	182

Estimates of Buyer Profits

- Estimating gains for data buyers is much more complex
  - Likelihood of ripping may be high
  - There is an expectation that not all data will be functional

- Estimates of direct funds acquired by identity thieves in the US in 2012
  - Credit card= ave.=$1,448; median= $300
  - Debit card= ave.=$552; median= $200

Estimated ROI: Dumps

- There were 117 instances of positive feedback from dumps sales
  - Assuming 65 cards are valid and active, the ROI varies based on what metric is used
    - Credit Card Loss Average
      - ($94,120-$10,260)/$10,260= 8.17 ROI
    - Credit Card Loss Median
      - ($19,500-$10,260)/$10,260= 0.9 ROI
  - Using the median loss, buyers could gain $2,281,500

Estimated ROI: Dumps

- There were 117 instances of positive feedback from dumps sales
  - Assuming 65 cards are valid and active, the ROI varies based on what metric is used
    - Debit Card Loss Average
      - ($35,880-$10,260)/$10,260= 2.49 ROI
    - Debit Card Loss Median
      - ($13,000-$10,260)/$10,260= 0.26 ROI
  - Using the median loss, buyers could gain $1,521,000

Estimated ROI: eBay/PayPal

- There is only one instance of positive feedback
  - Assuming 25 accounts are operational, the ROI is improved from that of dumps
    - Credit Card Loss Average
      - ($36,200-$1,362.50)/$1,362.50= 25.5 ROI
    - Credit Card Loss Median
      - ($7,500-$1,362.50)/$1,362.50= 4.5 ROI
    - Debit Card Loss Average
      - ($13,800-$1,362.50)/$1,362.50= 9.12 ROI
    - Debit Card Loss Median
      - ($5,000-$1,362.50)/$1,362.50= 2.66 ROI

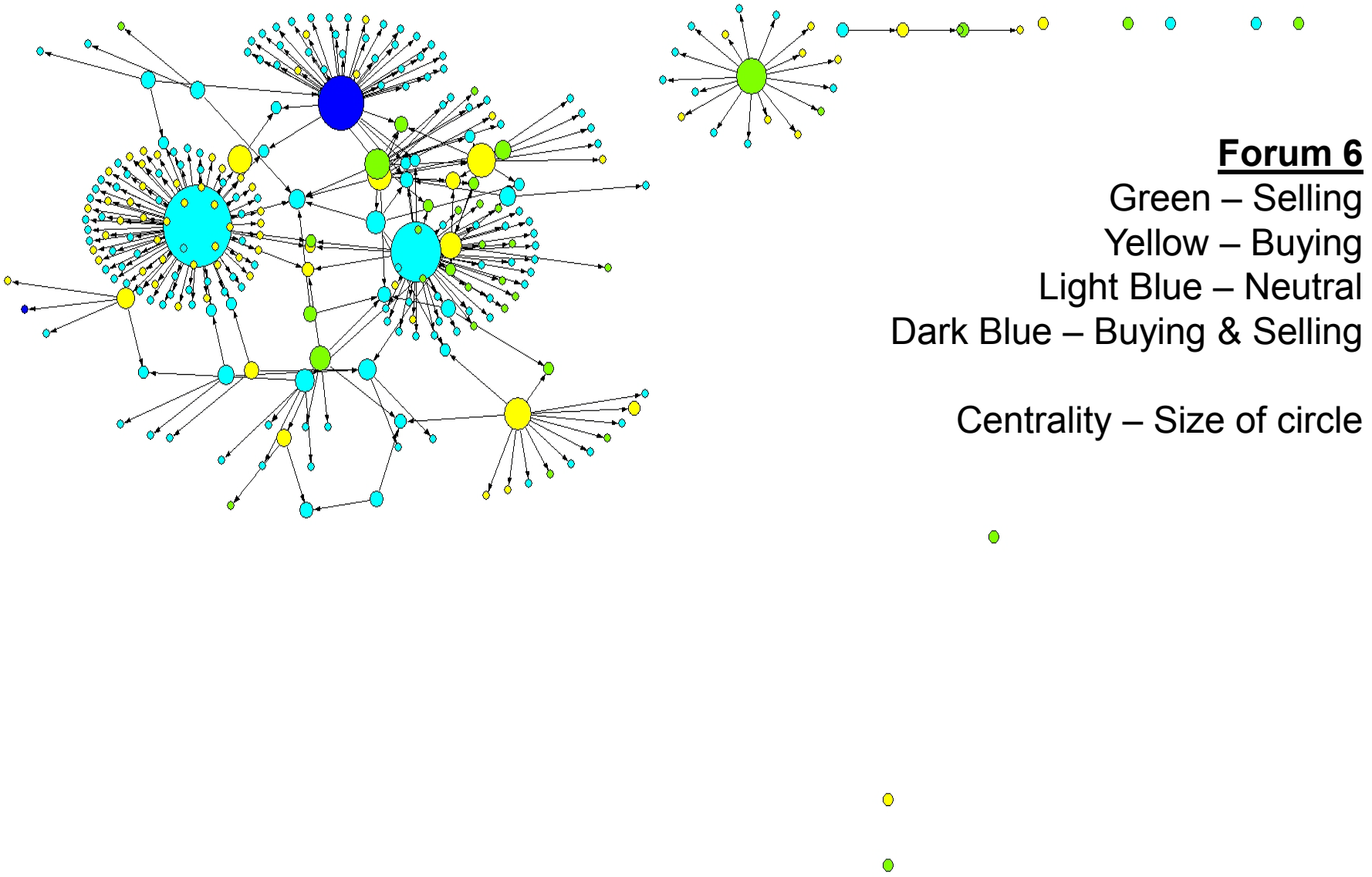
Forum SNA Descriptive Statistics

Forum	# of Threads	# of Users	# of Ties	# of Loops	Multiple Lines	Multiple Loops	Percent in the Largest Component
1	55	81	49	48	0	55	18.5
2	128	160	196	101	11	25	86.25
4	144	170	210	120	103	225	50.59
5	89	88	7	77	0	9	4.54
6	48	416	295	39	0	8	58.89
7	202	157	160	68	13	134	71.98
8	590	471	350	278	121	470	55.29
9	312	650	762	286	2	26	73.69
10	60	237	392	40	85	56	60.61
11	35	66	50	33	10	85	97.01
12	71	119	95	53	3	18	62.19
13	153	293	240	136	23	127	55.63

Forum Network Measures

Forum	Network Density	Average Degree	All Degree Centrality
1	0.016	2.568	7
2	0.013	4.163	8
4	0.023	7.741	15
5	0.012	2.114	11
6	0.002	1.644	11
7	0.015	4.777	17
8	0.006	5.266	54
9	0.003	3.346	10
10	0.010	4.835	1
11	0.041	5.394	19
12	0.012	2.840	7
13	0.006	3.283	13

Economic Activity By Centrality

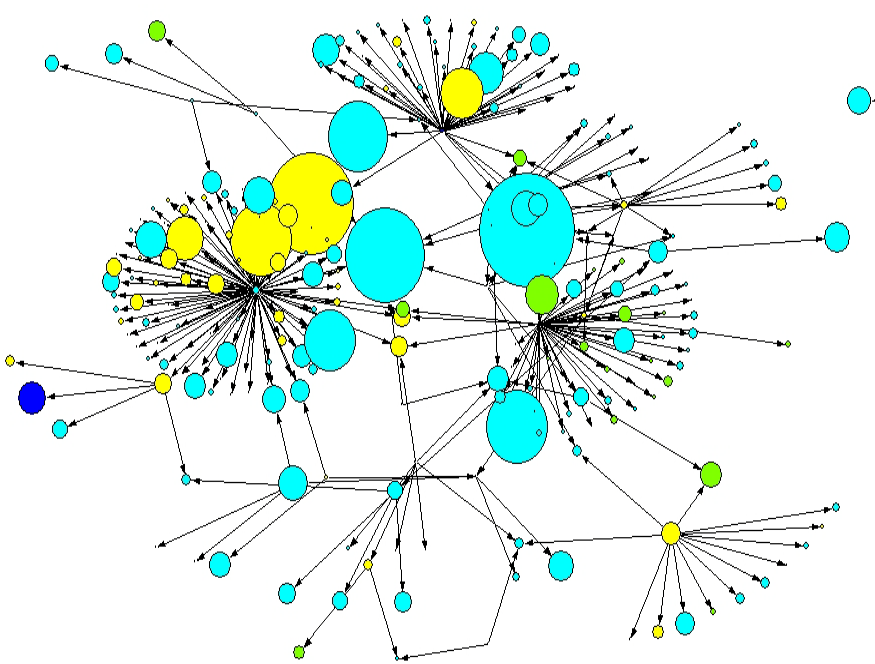


Forum 6

Green – Selling
Yellow – Buying
Light Blue – Neutral
Dark Blue – Buying & Selling

Centrality – Size of circle

Economic Activity by Post



Forum 6

Green – Selling

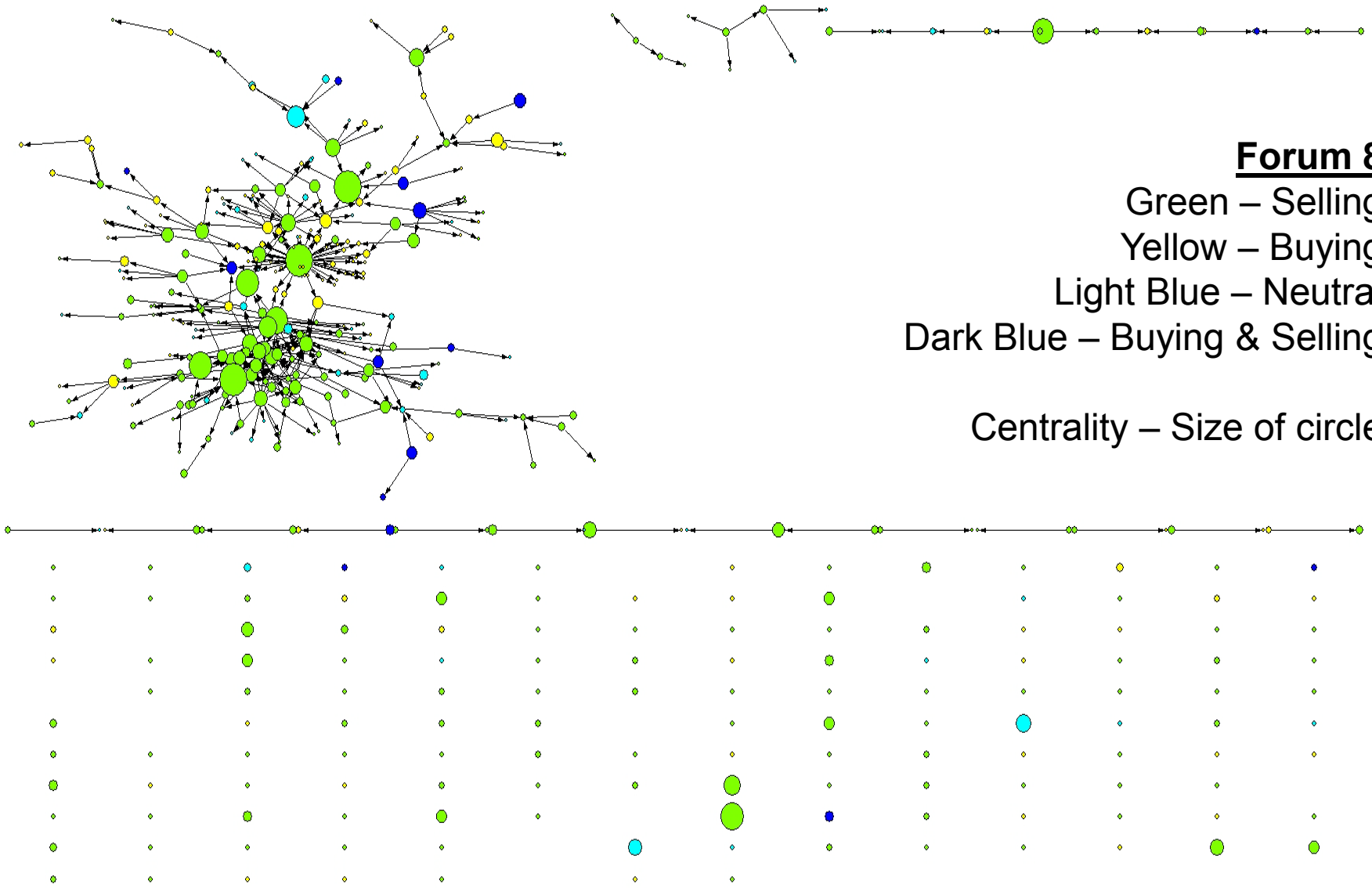
Yellow – Buying

Light Blue – Neutral

Dark Blue – Buying & Selling

Centrality – Size of circle

Economic Activity by Centrality



Forum 8

Green – Selling

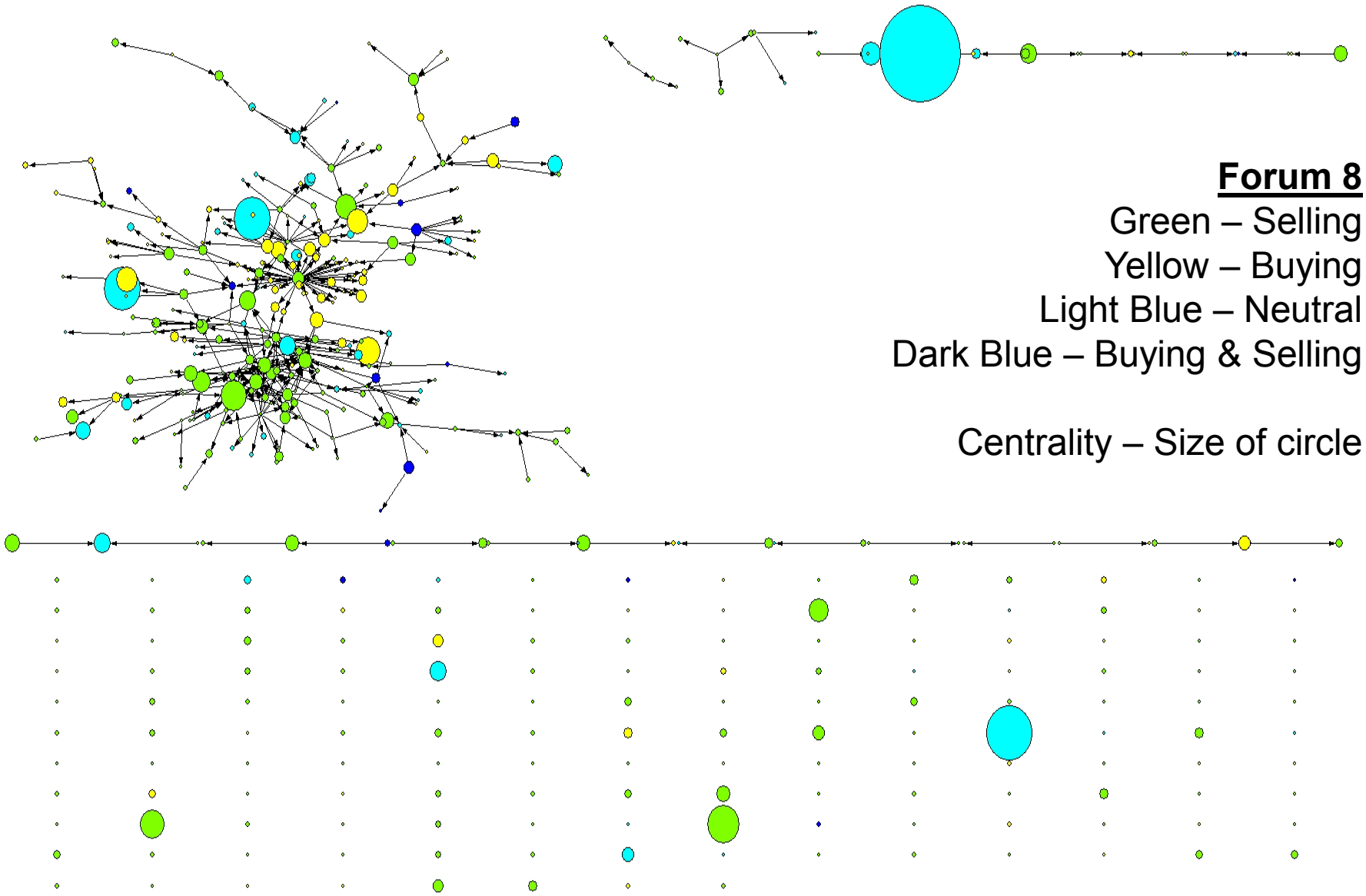
Yellow – Buying

Light Blue – Neutral

Dark Blue – Buying & Selling

Centrality – Size of circle

Economic Activity by Posts



Forum 8

Green – Selling

Yellow – Buying

Light Blue – Neutral

Dark Blue – Buying & Selling

Centrality – Size of circle

Discussion

- The forums appear to be organized at two levels
  - The sales process blurs the line between colleagues and peers
  - The forums comprise teams and formal organizations

- The network of stolen data markets are generally inefficient
  - Variations across stolen data markets based on centrality of users by status and participation

Market Disruption

- Based on our analyses, disruption should focus on the entire forum rather than individual sellers or Sybil attacks
  - Dark Market

- Pursue and prosecute payment services for their role in facilitating illicit transactions
  - Short term benefit, but long term impact

Evaluation and Partnerships

- There is a substantial need for law enforcement and academic partnerships
  - Vetted forums are the key vehicle but are closed off from general access
  - Evaluate and capture off-forum communications
  - Assess the impact of disruption methods on market operations

Further Research

- There is a need for substantial additional research
  - Data collection and analysis of various forums and IRC channels to validate findings
  - Data from either current or recently shut down PMs and ICQ communications to understand difference between advertised and negotiated price
  - Exploration of social network position relative to advertised price
  - Additional research on payment mechanisms and their influence on price

Questions?

- Please contact the PI:
- Dr. Thomas J. Holt
- Associate Professor
- Michigan State University
- holtt@msu.edu
- 517-353-9563