Buying Drugs for Science: Understanding the Economics of Cybercrime

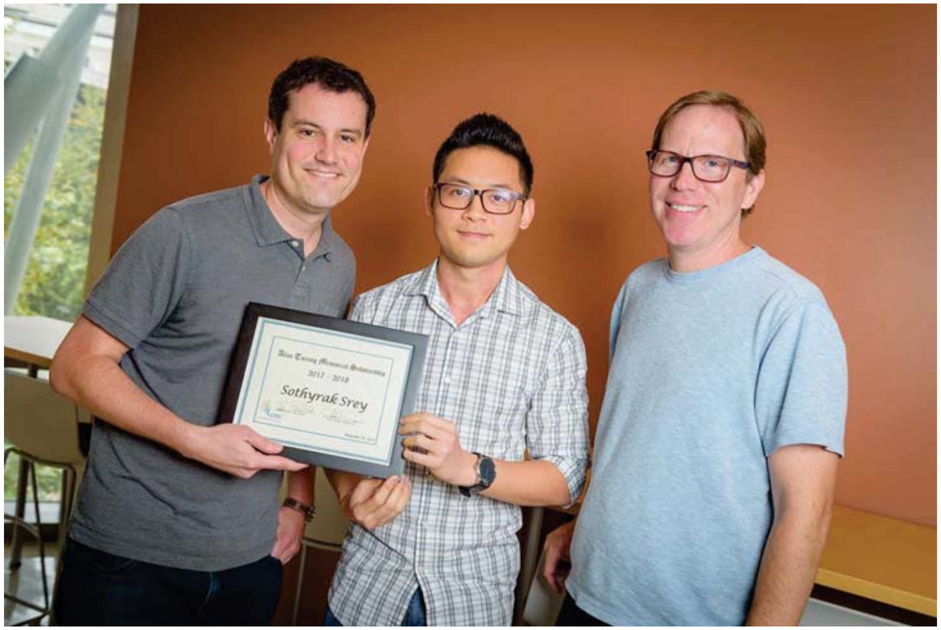
Stefan Savage
Center for Evidence-based Security Research
UC San Diego

joint work w/Neha Chachra, Brandon Enright, Mark Felegyhazi (ICSI), Chris Grier (Berkeley), Tristan Halvorson, Chris Kanich, Christian Kreibich (ICSI), Kirill Levchenko, He “Lonnie” Liu, Justin Ma, Damon McCoy, Vern Paxson (ICSI/Berkeley), Andreas Pitsillidis, Geoff Voelker, and Nick Weaver (ICSI)

Alan Turing Memorial Scholarship

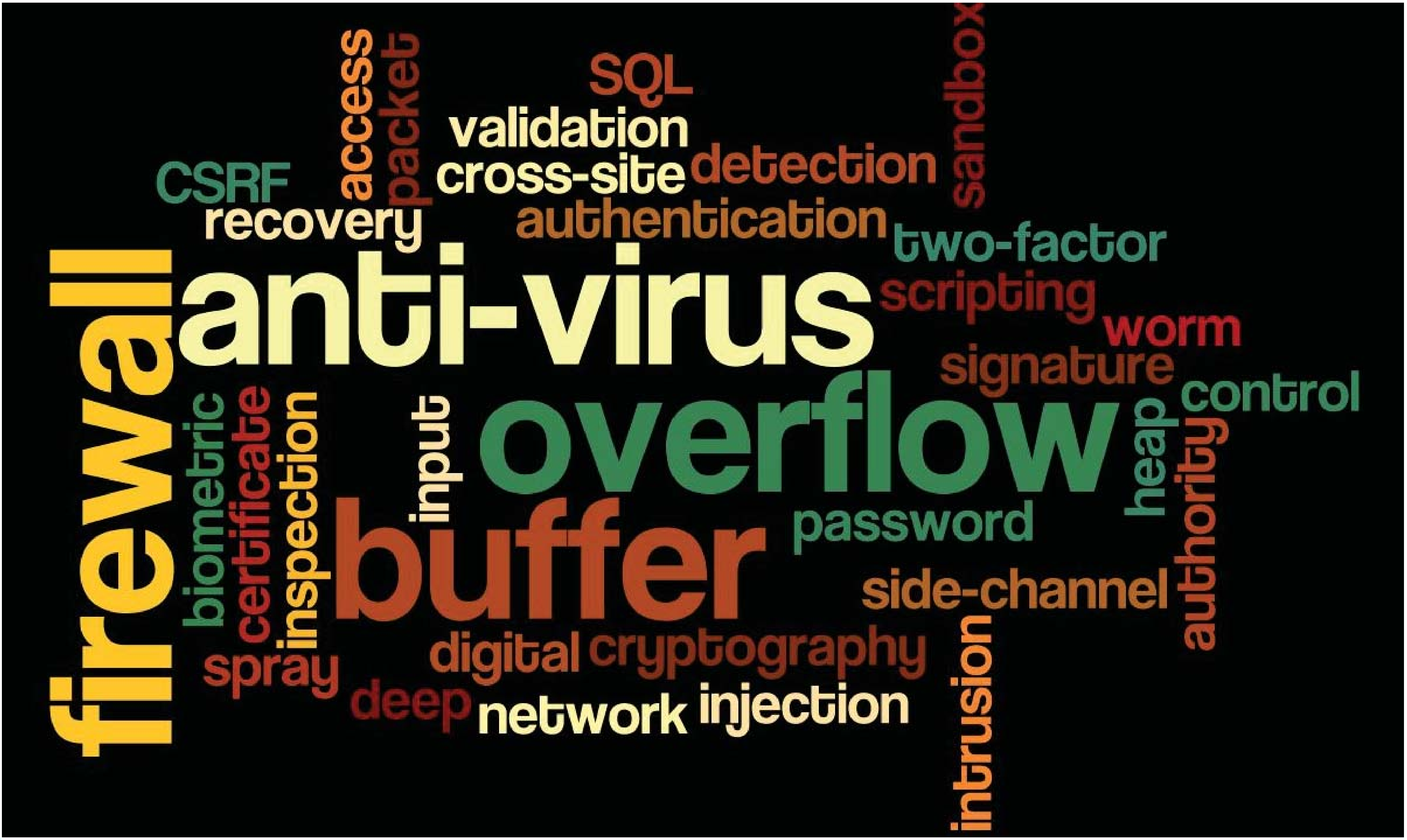
- Named for Alan Turing – father of computing

- Recognizes support for LGBT diversity efforts by students in CS & CE
- Working to raise $50k to endow this scholarship
- More info at: cns.ucsd.edu



2017 recipient Tee Srey

The traditional view of security…



A complementary viewpoint

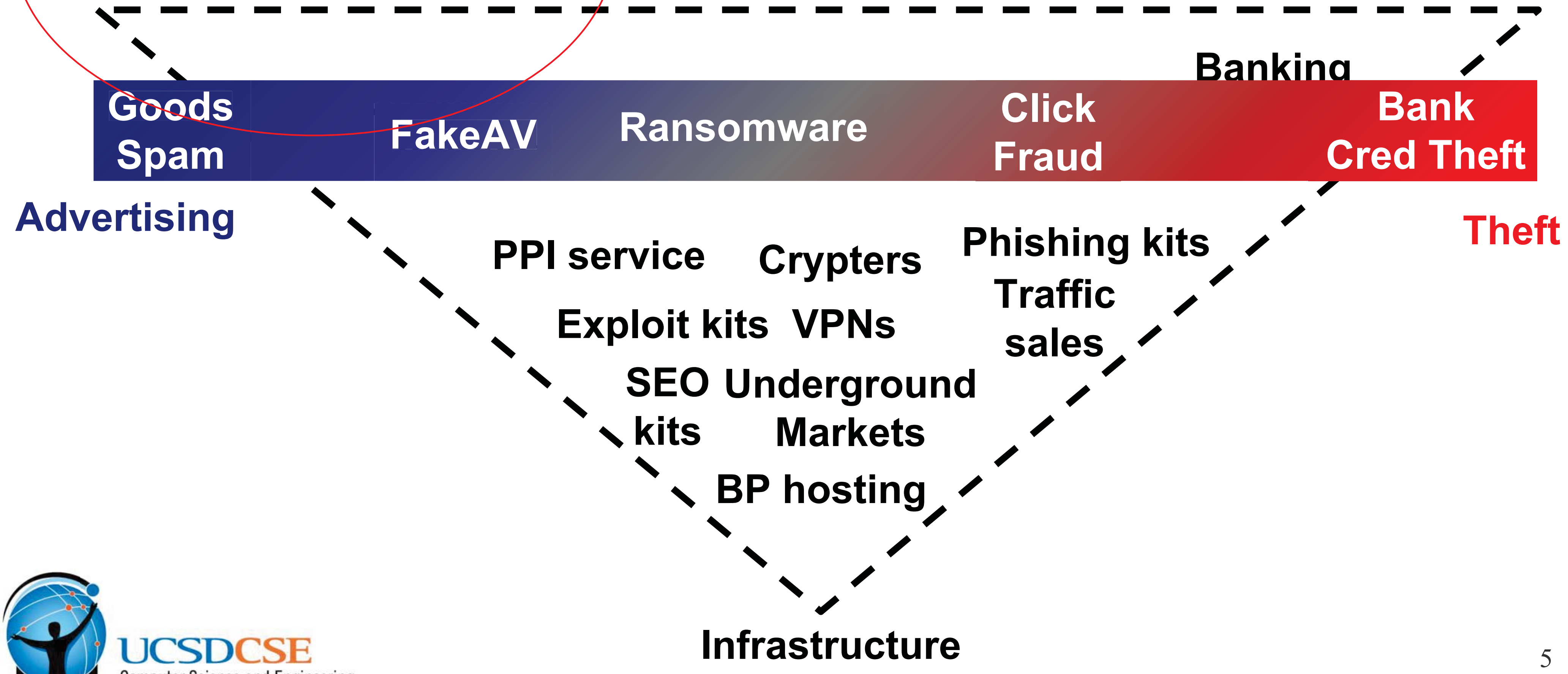
- There is a broader socio-economic context

  - **Actors**
    - Adversaries
    - Victims
    - Defenders
  - **Incentives/Costs**
  - **Capabilities**
  - **Relationships**

- Key hypothesis:
  - Understanding these factors will provide a more effective basis for designing security interventions

Economics of e-crime

- Today, the largest driver for threats is $$$
  - Scale allows commodity monetization



Goods Spam

FakeAV

Ransomware

Click Fraud

Banking

Bank Cred Theft

Advertising

Theft

PPI service

Crypters

Phishing kits

Traffic sales

Exploit kits

VPNs

SEO kits

Underground Markets

BP hosting

Infrastructure

UCSDCSE
Computer Science and Engineering

Today: Advertising-based e-crime

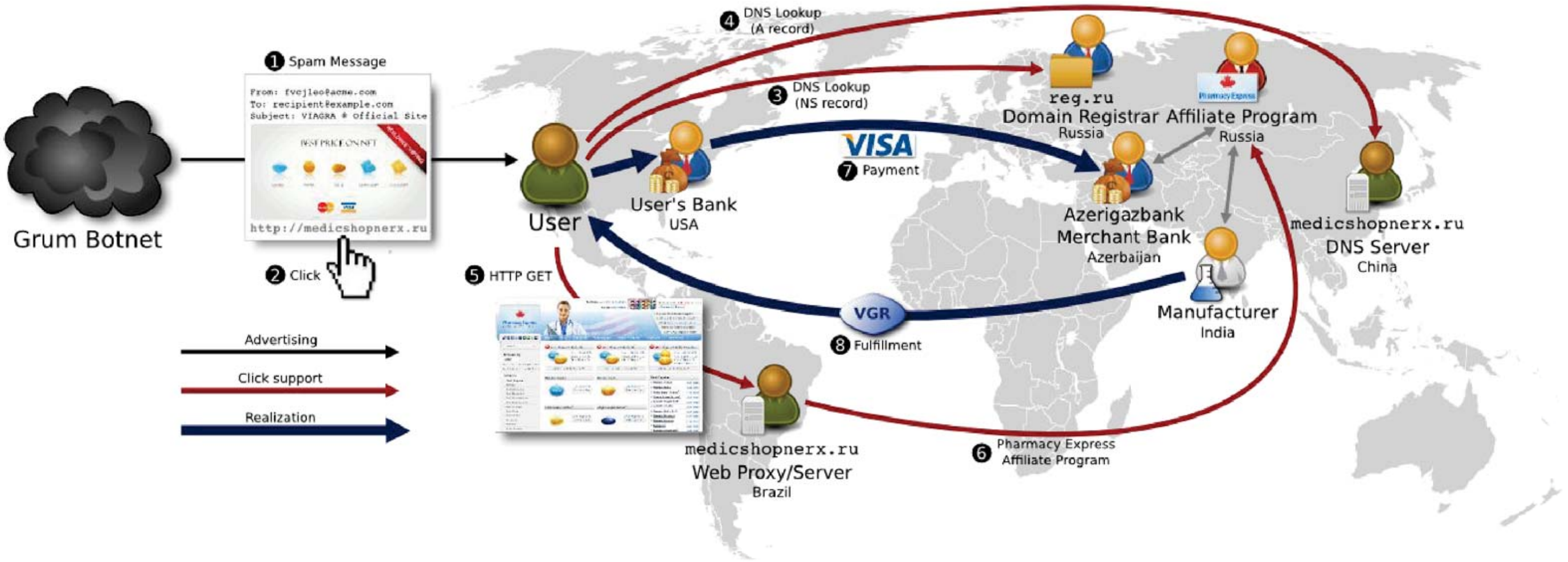
- Range of **abuse vectors** to reach consumer
  - E-mail spam, SEO, OSN abuse, blog spam, malware
- Range of **products/services advertised**
  - **Pharma**, replica luxury goods, apparel and electronics, pirated movies, music, books and **software**, diplomas, dating, porn, gambling
  - FakeAV
- Almost all use an **affiliate marketing structure**
- Key point: monetized ***directly*** by consumers

Affiliate program structure

- Division of labor
  - **Affiliates** handle advertising (e.g., spam, SEO)
    - Independent contractors
    - Paid 25-60% commission depending on program
  - **Affiliate programs** handle backend
    - Payment processing, customer service, fulfillment
    - Sometimes hosting and domain registration
- Why?
  - Transfer of risk: innovation risk vs investment risk
  - Specialization lowers cost structure

One such example: Pharmaceutical e-mail spam

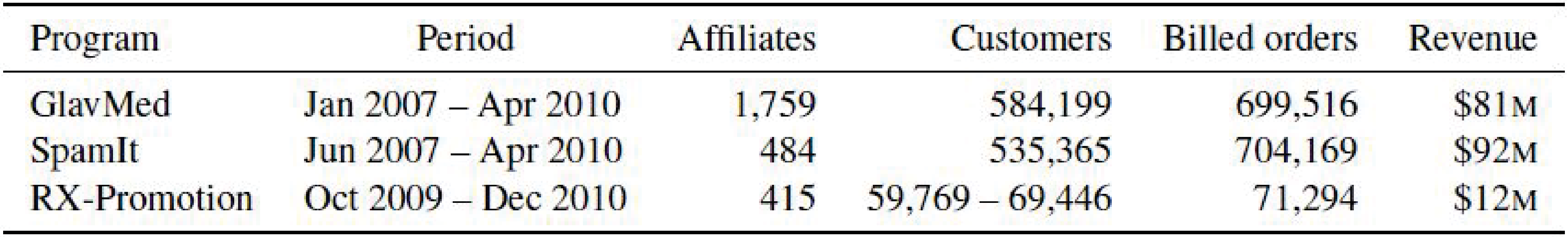
- Complex value chain relationships



From: fvcjleo@acme.com
To: recipient@example.com
Subject: VIAGRA ® Official Site

A quick look inside a criminal pharmaceutical business

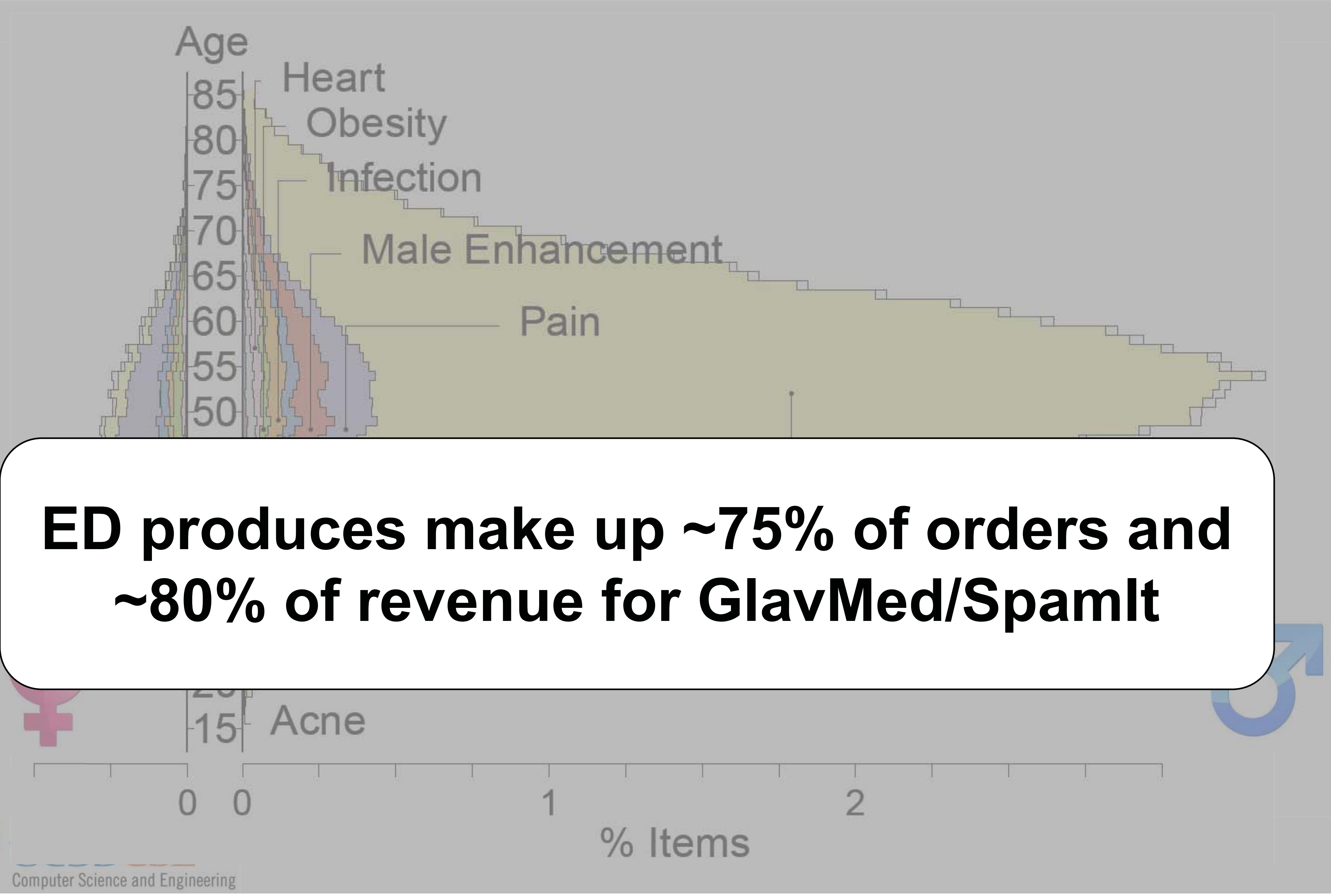
- Case study: Glavmed/Spamit, Rx-Promotion
  - 185M in gross revenue, 1+ million customers, 1.5+ million purchases, 2600+ affiliates
  - **75% of customers from US, 91% from West**



Program	Period	Affiliates	Customers	Billed orders	Revenue
GlavMed	Jan 2007 – Apr 2010	1,759	584,199	699,516	$81M
SpamIt	Jun 2007 – Apr 2010	484	535,365	704,169	$92M
RX-Promotion	Oct 2009 – Dec 2010	415	59,769 – 69,446	71,294	$12M

McCoy, Pittsillidis, Jordan, Weaver, Kreibich, Krebs, Voelker, Savage, Levchenko, *Pharmaleaks: Understanding the Business of Online Pharmaceutical Affiliate Programs*, USENIX Sec 2012

Product purchase demographics



ED produces make up ~75% of orders and ~80% of revenue for GlavMed/SpamIt

Demand drivers

- Embarrassment/Taboo (80+% revenue is ED)
  - "Lifestyle" drugs (some ED, hair loss, diet, acne)

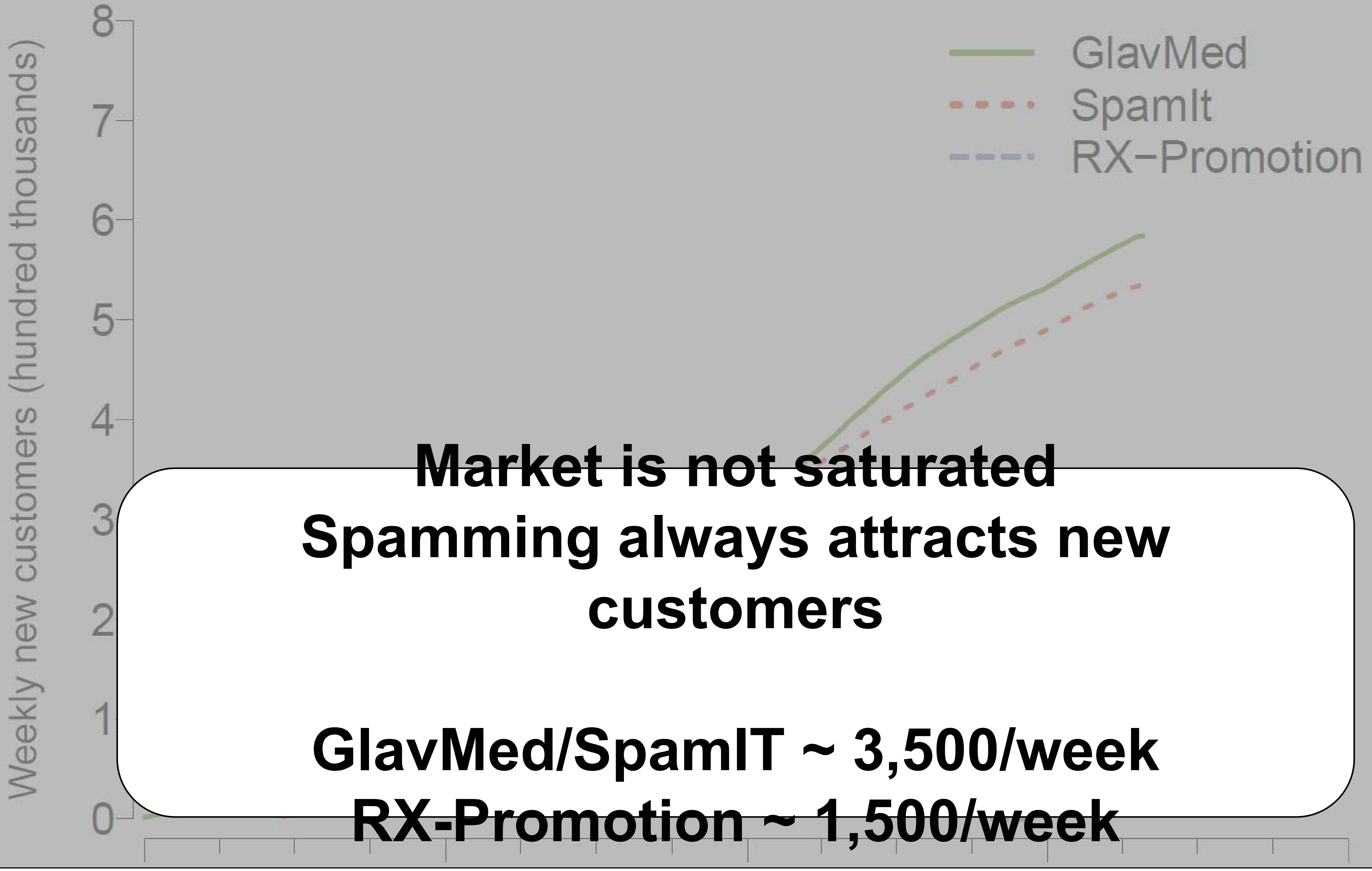
Spam filtering doesn't stop demand

20-40% of all sales come *from* the Spam folder

- Lack of legitimate market
  - Male enhancement, weird formulations (VSF)

UCSDCSE
Computer Science and Engineering

New customers over time (why spamming works)



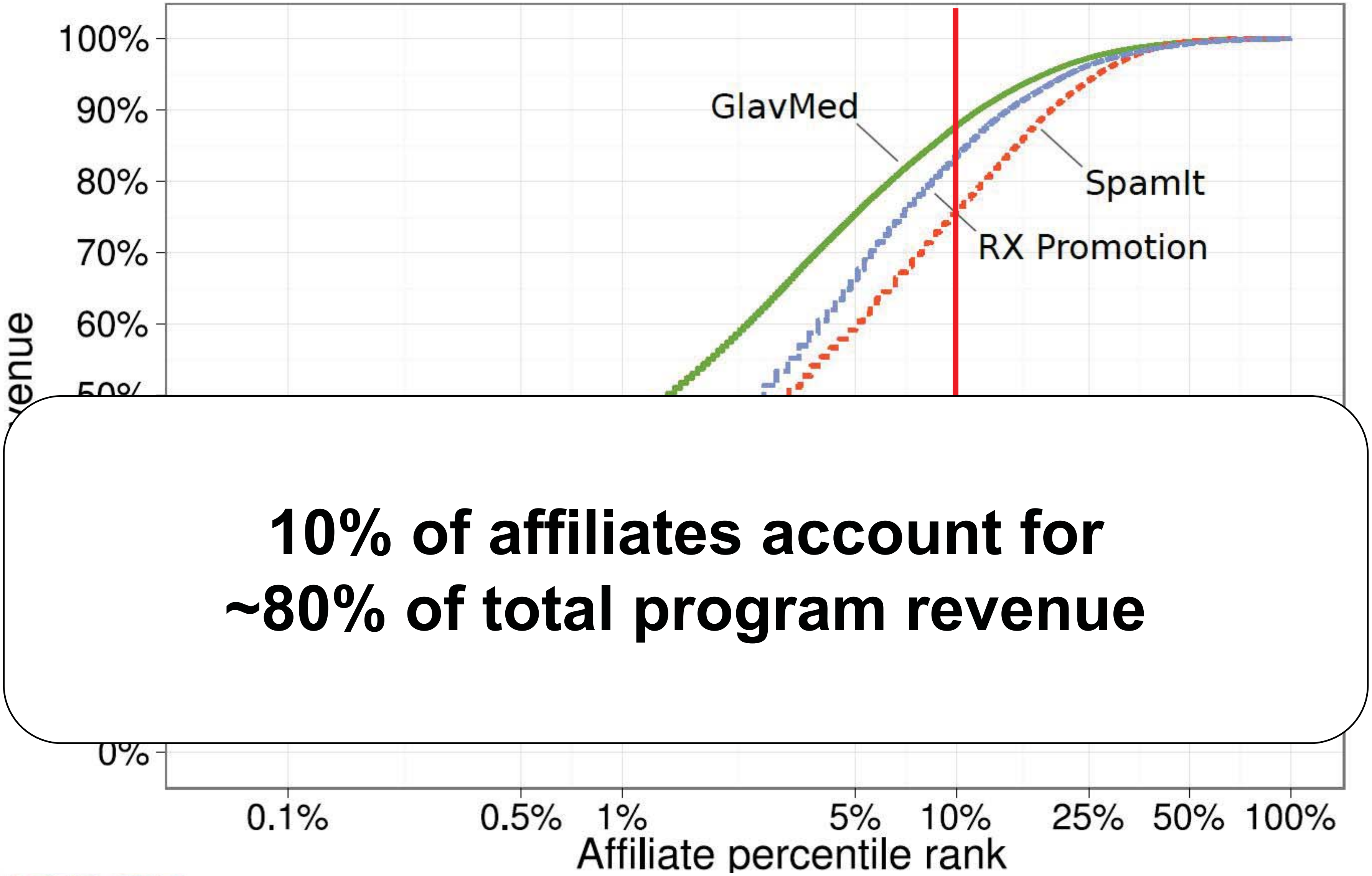
Market is not saturated

Spamming always attracts new customers

GlavMed/SpamIT ~ 3,500/week

RX-Promotion ~ 1,500/week

Affiliates Revenue



10% of affiliates account for ~80% of total program revenue

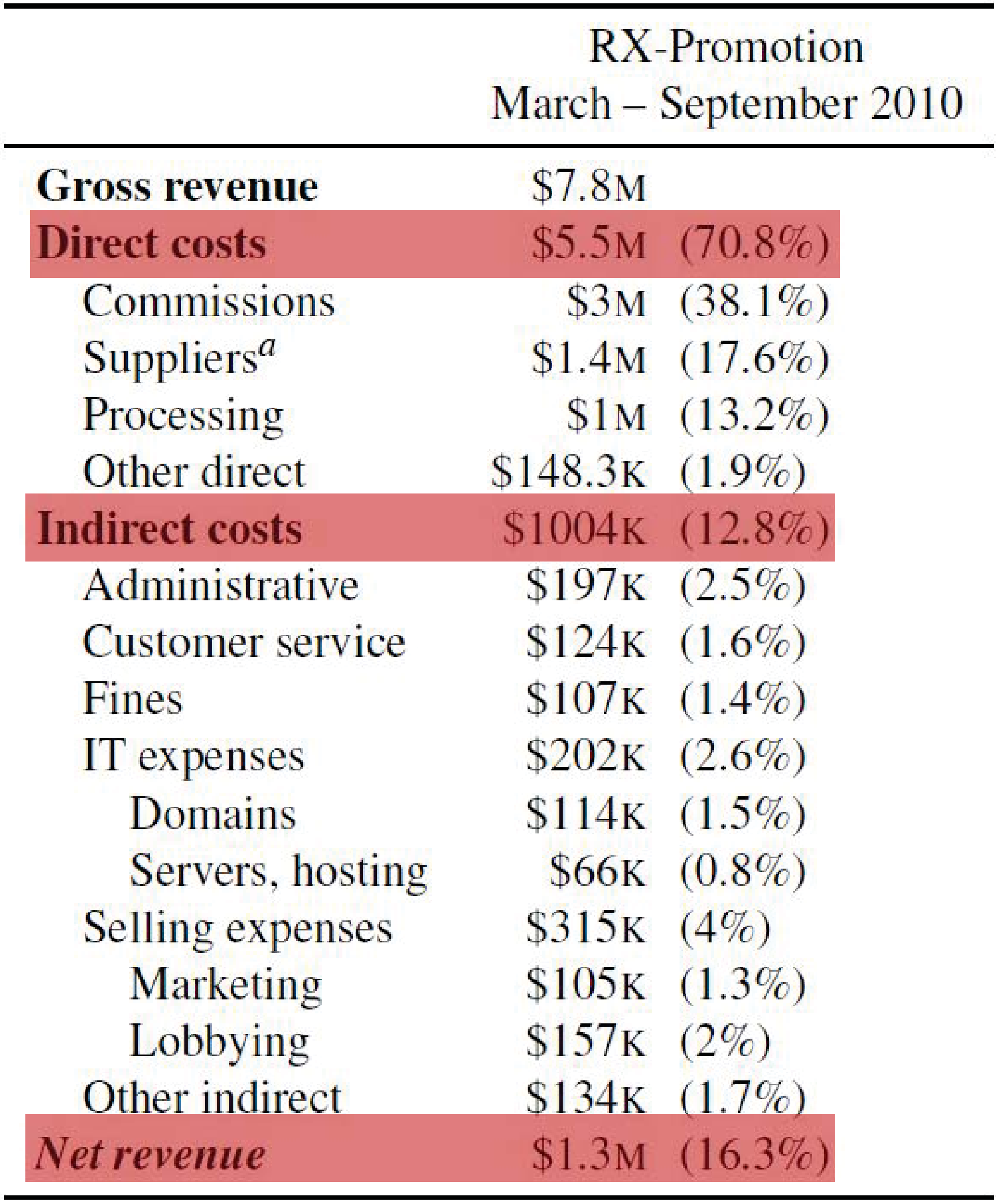
UCSDCSE
Computer Science and Engineering

Business model (for affiliate program)

- Brilliant business model, risk transference
  - Advertising liabilities and innovation cost -> advertisers
  - Low switching cost on both sides
- Rough cost structure
  - Direct costs (~70-75%) + 10% Holdback risk
    - C: Commissions to advertisers (~ 0.30-0.45)
    - S: Supply cost (~0.15-20; **dominated by shipping**, goods~6-7%)
    - P: Payment processing overhead (~0.10-0.15; 3-5% refund)
  - Indirect costs (~6-12%)
- Gross margins = ~ 10-20%

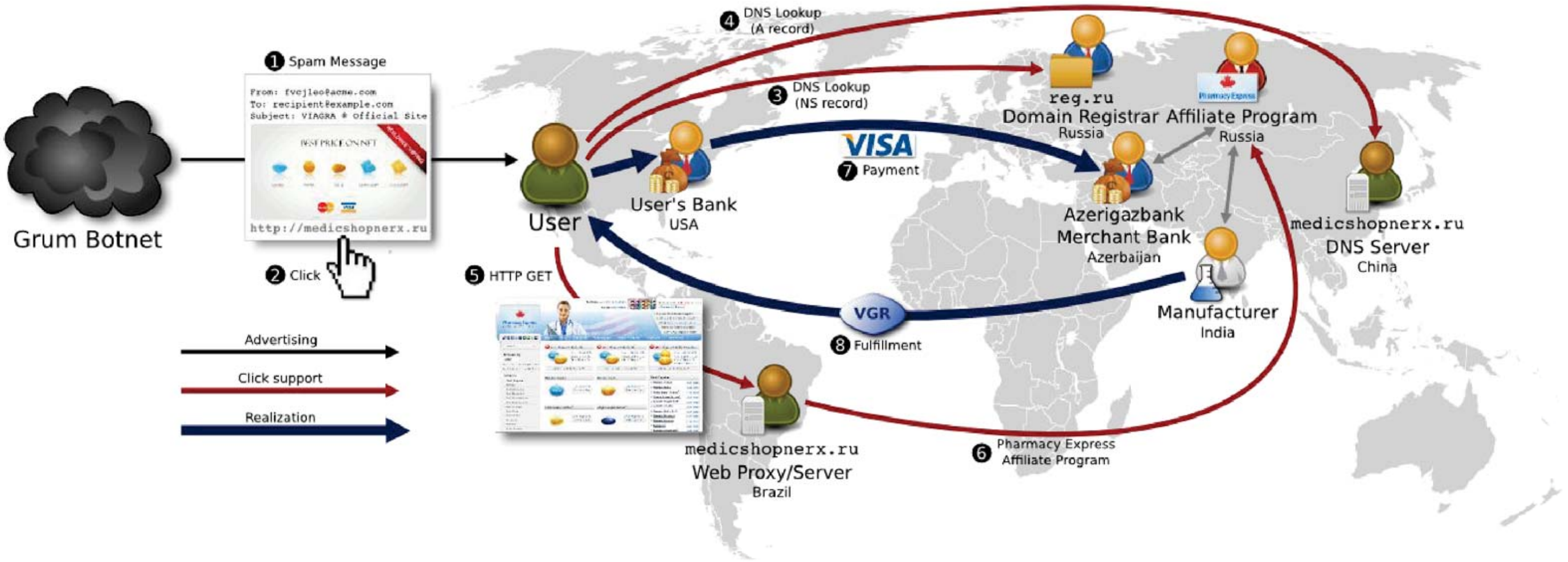
Affiliate program cost structure concrete example: RX-Promotion

Direct costs: 70.8%
Indirect costs: 12.8%
Profit: 16.3%



	RX-Promotion March – September 2010	
Gross revenue	$7.8M	
Direct costs	$5.5M	(70.8%)
Commissions	$3M	(38.1%)
Suppliers[a]	$1.4M	(17.6%)
Processing	$1M	(13.2%)
Other direct	$148.3K	(1.9%)
Indirect costs	$1004K	(12.8%)
Administrative	$197K	(2.5%)
Customer service	$124K	(1.6%)
Fines	$107K	(1.4%)
IT expenses	$202K	(2.6%)
Domains	$114K	(1.5%)
Servers, hosting	$66K	(0.8%)
Selling expenses	$315K	(4%)
Marketing	$105K	(1.3%)
Lobbying	$157K	(2%)
Other indirect	$134K	(1.7%)
Net revenue	$1.3M	(16.3%)

Where to intervene?



From: fvcjleo@acme.com
To: recipient@example.com
Subject: VIAGRA ® Official Site

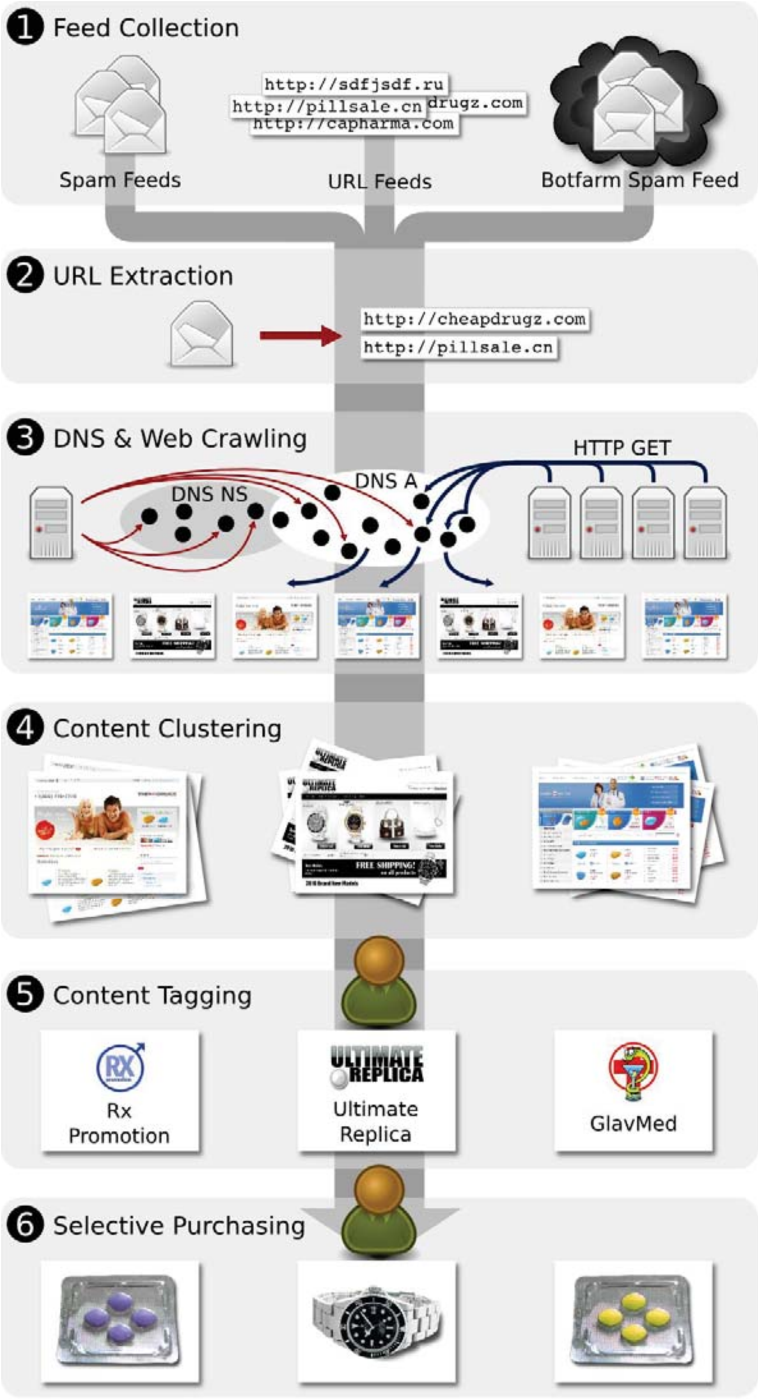
BEST PRICE ON NET

http://medicshopnerx.ru

Click Trajectory project

- Key idea
  - Find “bottlenecks” in the full spam value chain
  - Place where intervention could be most effective
    - **Eliminating resources has largest impact on profitability**
    - **Fewest alternatives, highest switching cost for adversary**
- Measure empirically
  - Resources needed to monetize each piece of spam
  - By playing the role of customer; at scale
    - Three domains: pharma, replica, software

Levchenko, Pitsillidis et al,
Click Trajectories: End-to-end analysis of the Spam value chain, IEEE S &P, 2011



- Click Trajectories study [Levchenko, IEEE S&P 2011]
- Goal: identify key **bottlenecks** in spam value chain

- 7 URL/Spam feeds + 5 botnet feeds
  - 968M URLs, 17M domains
  - 99% of pharma, OEM, replica
- Crawled domains for 98% of URLs
- Hundreds of purchases
  - **Unique card # per order**
  - **Full transaction data**

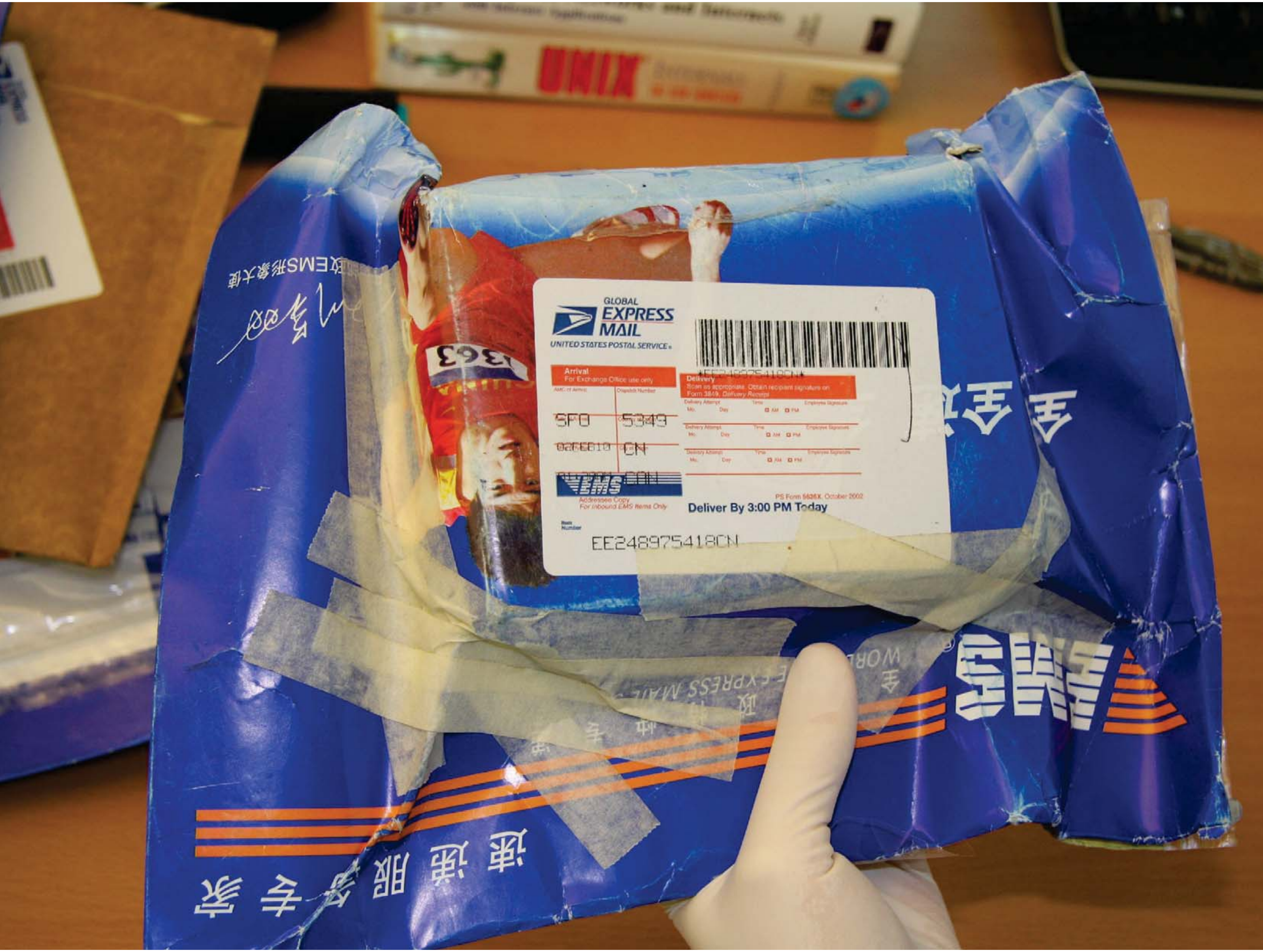
What is gained by purchasing?

- Insight into **realization** phase
  - **Fulfillment**
    - Receiving anything?
    - Where shipped from?
    - Contents of order?
  - **Payment info** (*via relationship with card issuers*)
    - Bank Identification Number (BIN) of **acquiring** bank
    - Merchant descriptor
    - Card Acceptor ID (CAID) (MID + TID)
    - Merchant Category Code (MCC)

UCSDCSE
Computer Science and Engineering

Director of
purchasin
g

Project
lead



GLOBAL EXPRESS MAIL
UNITED STATES POSTAL SERVICE®

EE248975418CN

Arrival
For Exchange Office use only

AMC of Arrival	Dispatch Number
SFO	5349
02FEB10	CN

Delivery
Scan as appropriate. Obtain recipient signature on Form 3849, *Delivery Receipt*

Delivery Attempt	Time	Employee Signature
Mo. Day	□ AM □ PM	
Mo. Day	□ AM □ PM	
Mo. Day	□ AM □ PM	

EMS
Addressee Copy
For Inbound EMS Items Only

PS Form 5626X, October 2002

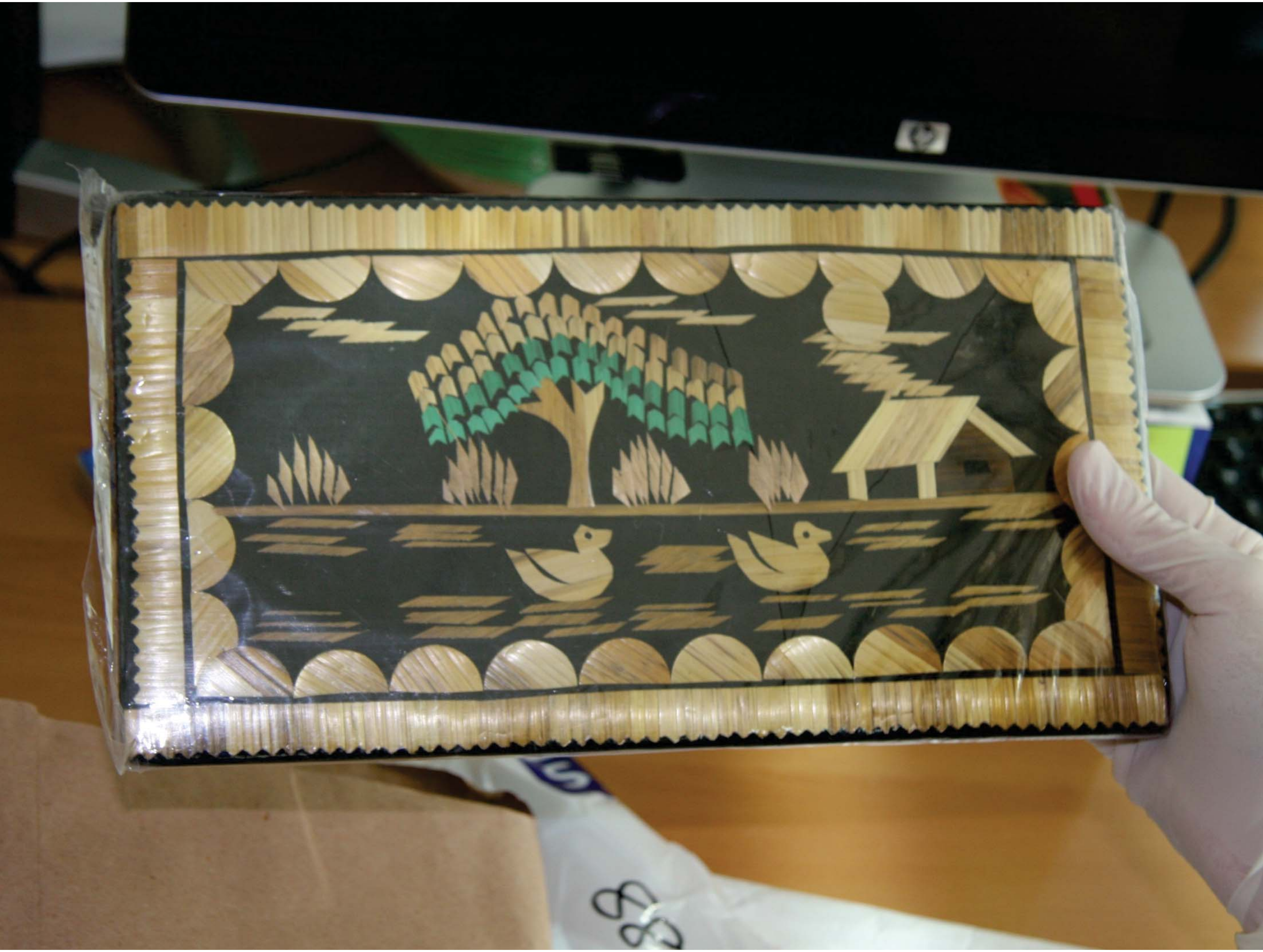
Deliver By 3:00 PM Today

Item Number
EE248975418CN

ROLEX
OYSTER PERPETUAL DATE
SUBMARINER
1000ft=300m
SUPERLATIVE CHRONOMETER
OFFICIALLY CERTIFIED
16
10
20
30
40
50

SEALED FOR YOUR PROTECTION
vpXl
#1 Dietary Supplement for Men
100% Natural Dietary Supplement
Contains 60 capsules
hank you for using
ge required

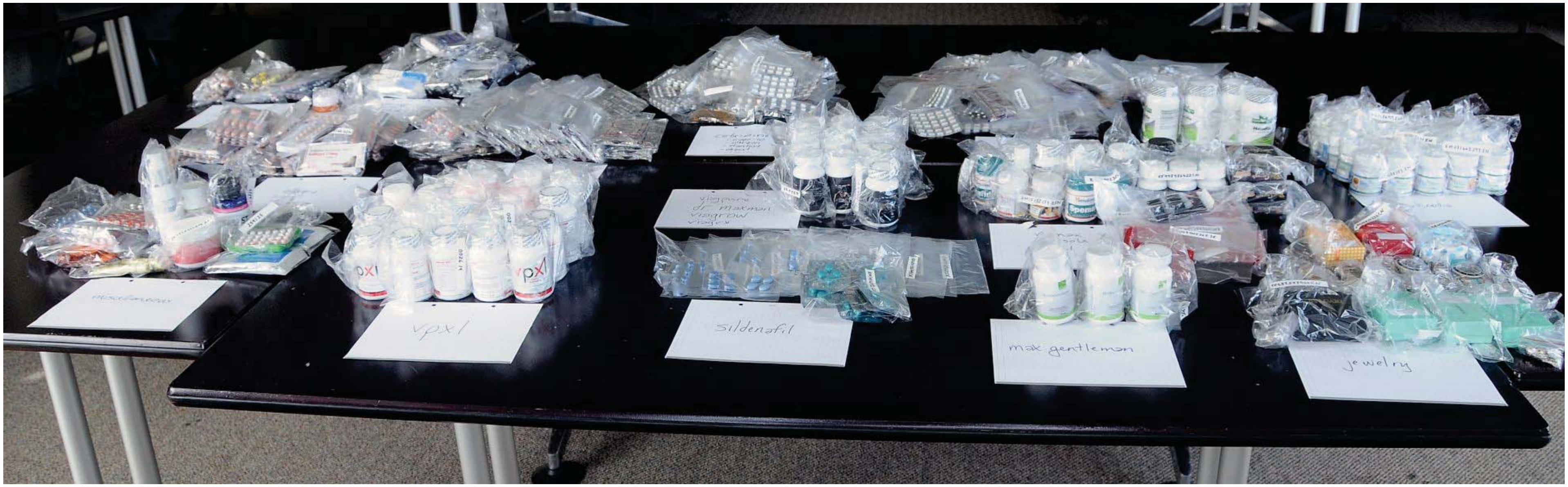
EXPRESS MAIL
6726635IN
DECLARATION EN DOUANE
SUPPLIERS
Kunj, Plot No. 214B,
ad, Andheri (W).
MEDICINE
Pill72
Cipla


88

USA
Kores
32122
USA.
8393597
FREIGHT
FREIGHT AIRPORT-TO-AIRPORT

351 1 A
S ENCLOSED
880654
USA
Express

600+ orders later…



Aside: not a fraud game

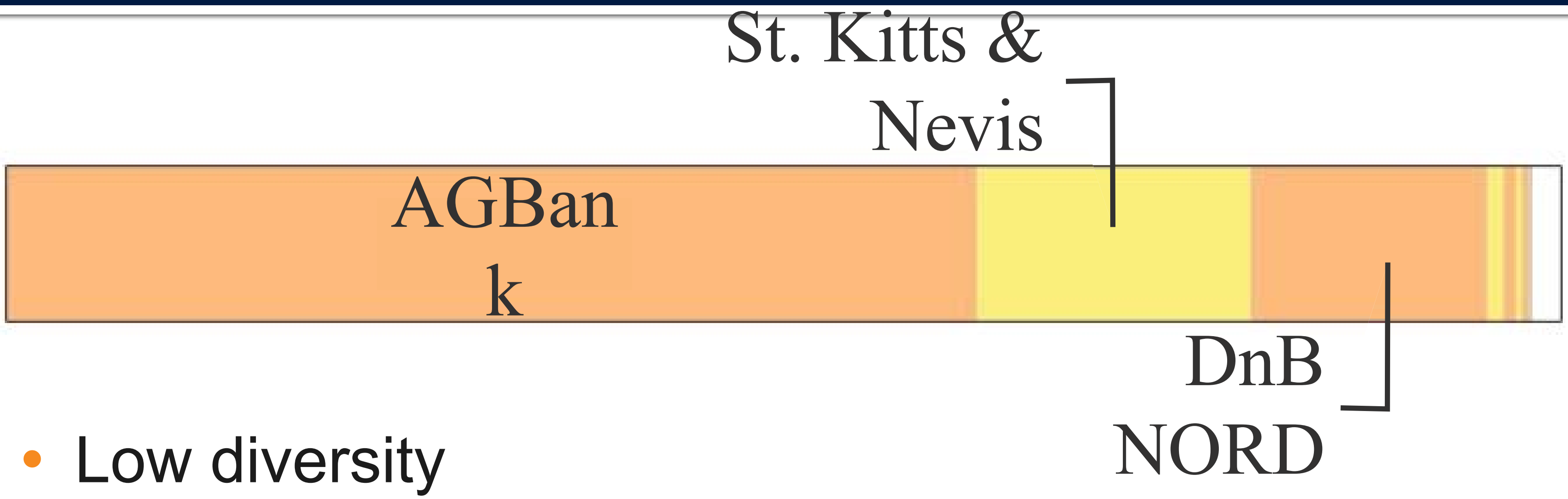
- We've made many hundreds of orders now
  - Pharma, herbal, replica, software, fakeAV
  - Shipment for all but one
  - Basically no fraud losses on cards (exceptions: data breach of Glavmed, 1 FakeAV)
- Significant **reorder business** (~30%)
  - Need to keep customers happy
- Affiliate programs generally *believe* they are selling reasonable quality goods

The bad news

- Most resources are cheap and plentiful
  - Registrars, name servers, Web hosting
- Replacement cost < expected profit
  - Examined blacklisting, filtering, takedown, etc… all have *little revenue impact*
  - May protect customers, but doesn't undermine business model

- **One major exception**…

Merchant banks (circa 2010)



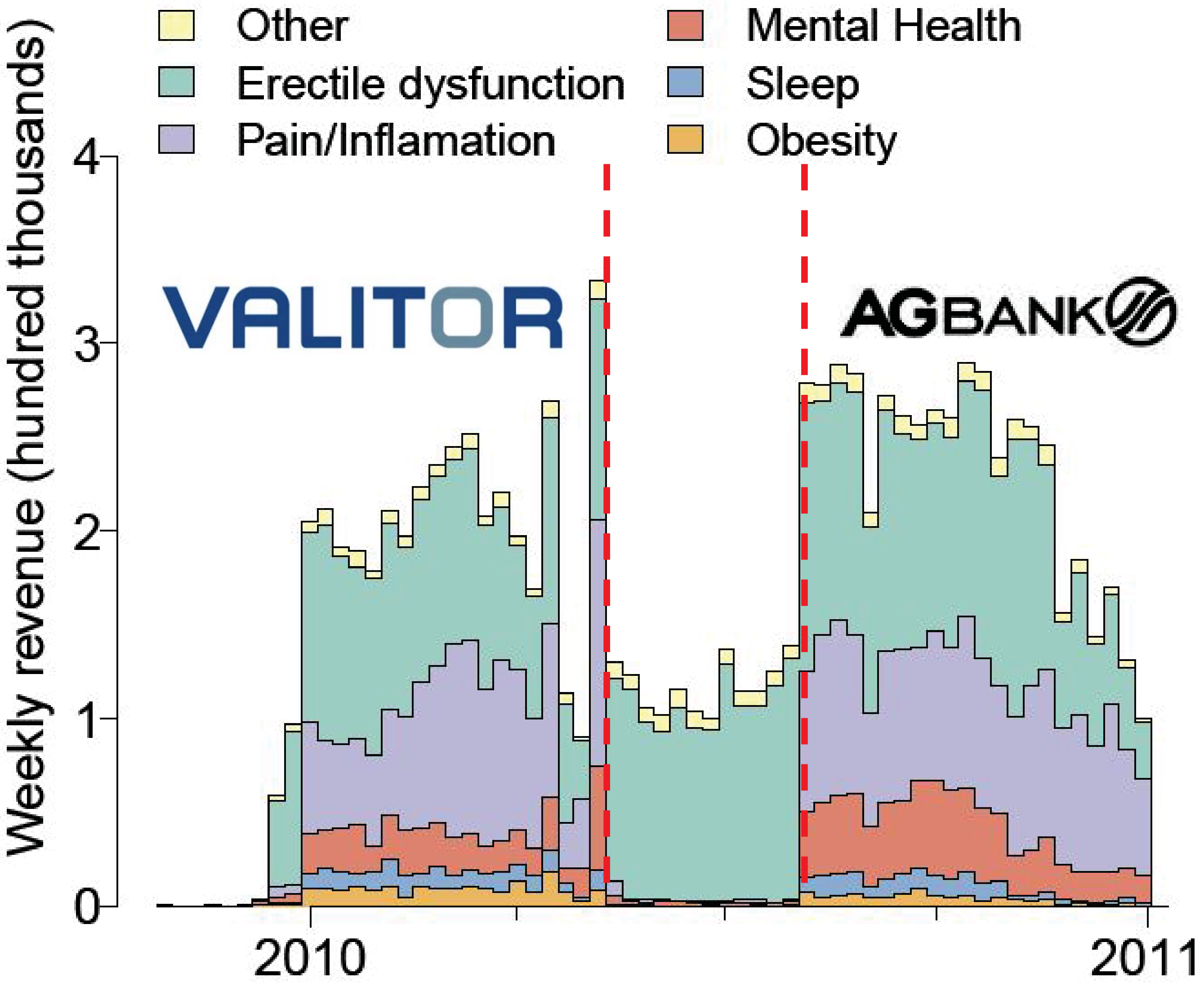
- Low diversity
  - 3 banks covered 95% of spam
  - Fewer banks willing handle “high-risk” merchants
- High switching cost
  - In-person account creation, due diligence, multi-day process
  - Upfront capital, holdback forfeiture

UCSDCSE
Computer Science and Engineering

Hypothesis

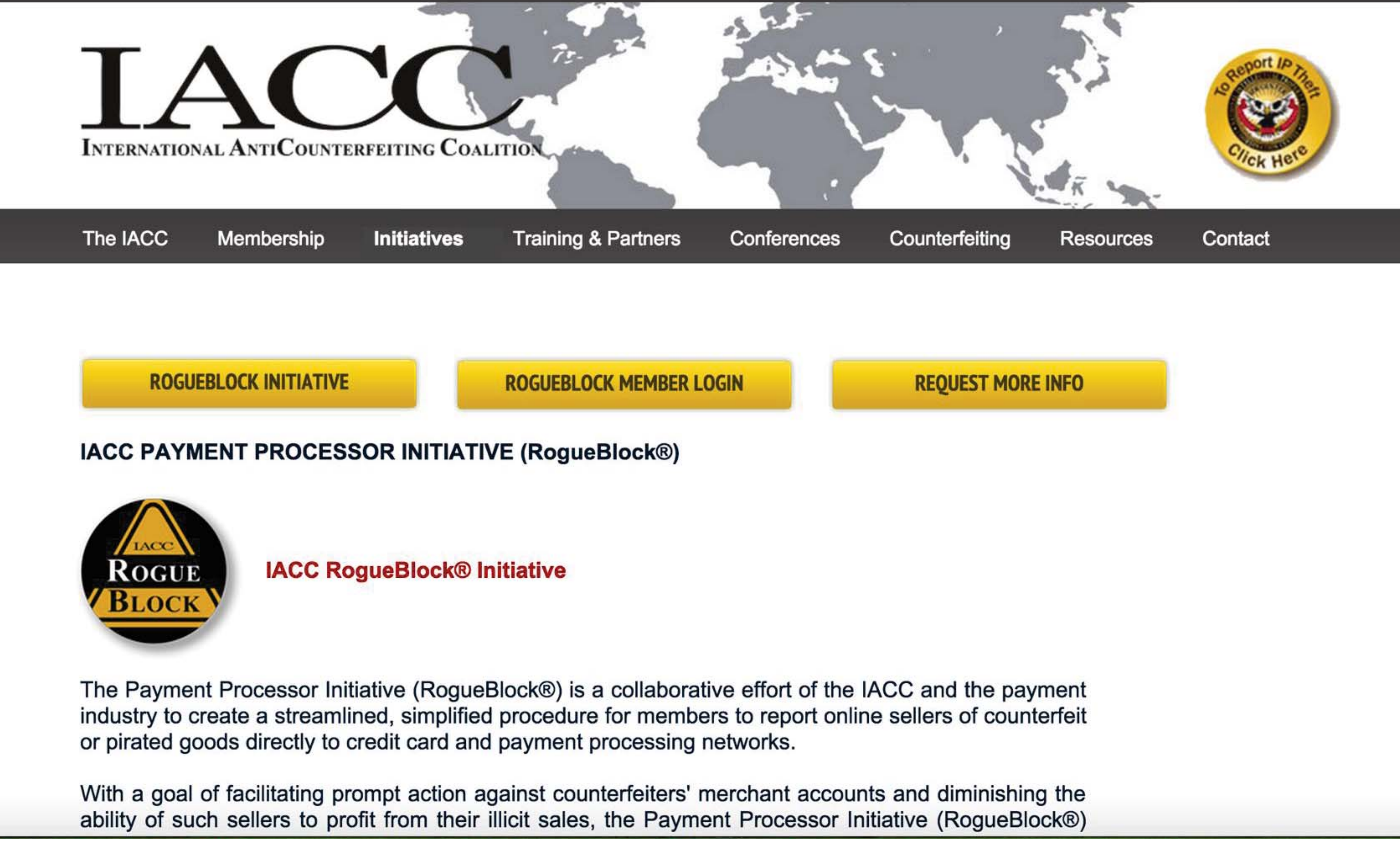
- If we could target merchant accounts…
  - Could demonetize entire system
  - Asymmetry that favors the good guys!

Anecdotal evidence:
Revenue by drug type (RX-Promo)



UCSDCSE
Computer Science and Engineering

A brief tech transfer story



IACC PAYMENT PROCESSOR INITIATIVE (RogueBlock®)

IACC RogueBlock® Initiative

The Payment Processor Initiative (RogueBlock®) is a collaborative effort of the IACC and the payment industry to create a streamlined, simplified procedure for members to report online sellers of counterfeit or pirated goods directly to credit card and payment processing networks.

With a goal of facilitating prompt action against counterfeiters' merchant accounts and diminishing the ability of such sellers to profit from their illicit sales, the Payment Processor Initiative (RogueBlock®)

Result: targeted payment intervention efforts today

- **Undercover** test purchase at counterfeit site
  - Get merchant bank BIN from transaction
- IP holder notifies card network (e.g., Visa/MC)
  - Investigation; complaint delivered to merchant bank
- **Leverage via card association contract**
  - Merchant bank owns liability
  - Fines, increased scrutiny, de-association
- Merchant account shutdown

So… does it work?

- Bottom line: **Yes, amazingly well.**
- We've tracked bank association w/affiliate programs for almost two years (continuing…)
  - ~1000 purchases (Visa only)
- Joined programs as affiliates to get damage assessment from inside
- Quick stories: OEM software and Pharma

McCoy, Dharmdasani, Kreibich, Voelker and Savage,
Priceless: The Role of Payments in Abuse-advertised Goods, ACM CCS 2012

Example: OEM (pirate) software

cdrbsoftware
Affordable Software Titles

По вопросам регистрации и суппорта обращаемся смело 371-777

OEMCash

SOFT MONSTER

ПРИВАТНАЯ OEM-ПАРТНЁРКА – СИЛА!
ВЫСОКИЙ КОНВЕРТ
БОЛЬШОЙ ВЫХЛОП!

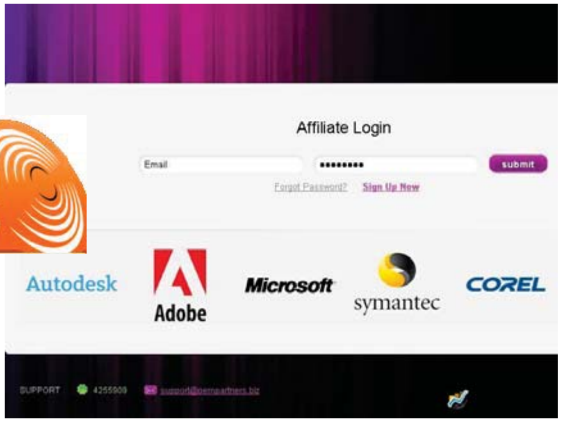
WAREZSTORE.COM

software sellers

OEM Soft Store
Easy and Fast Download

OEM 2012

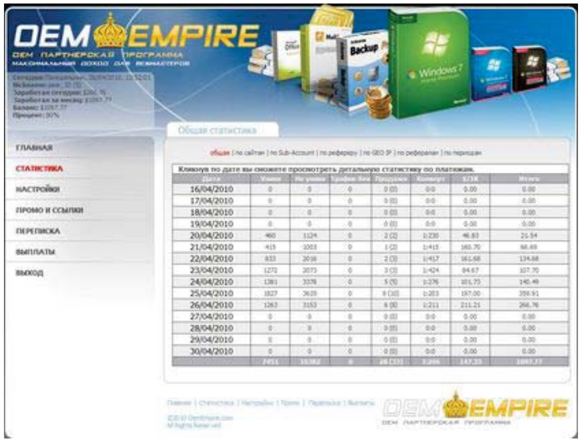
SOFT SALES



Affiliate Login

Email ••••••••

SUPPORT 4255909 support@oempartners.biz



Сегодня: Понедельник, 26/04/2010, 11:52:01
Заработал сегодня: $266.76
Заработал за месяц: $1097.77
Баланс: $1097.77
Процент: 50%

Общая статистика

общая | по сайтам | по Sub-Account | по рефереру | по GEO IP | по рефералам | по периодам

Кликнув по дате вы сможете просмотреть детальную статистику по платежам.

Дата	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
16/04/2010	0	0	0	0 (0)	0:0	0.00	0.00
17/04/2010	0	0	0	0 (0)	0:0	0.00	0.00
18/04/2010	0	0	0	0 (0)	0:0	0.00	0.00
19/04/2010	0	0	0	0 (0)	0:0	0.00	0.00
20/04/2010	460	1124	0	2 (2)	1:230	46.83	21.54
21/04/2010	415	1003	0	1 (2)	1:415	160.70	66.69
22/04/2010	833	2016	0	2 (3)	1:417	161.68	134.68
23/04/2010	1272	2073	0	3 (3)	1:424	84.67	107.70
24/04/2010	1381	3376	0	5 (5)	1:276	101.75	140.49
25/04/2010	1827	3635	0	9 (10)	1:203	197.00	359.91
26/04/2010	1263	3153	0	6 (6)	1:211	211.21	266.76
27/04/2010	0	0	0	0 (0)	0:0	0.00	0.00
28/04/2010	0	0	0	0 (0)	0:0	0.00	0.00
29/04/2010	0	0	0	0 (0)	0:0	0.00	0.00
30/04/2010	0	0	0	0 (0)	0:0	0.00	0.00
	7451	16382	0	28 (31)	1:266	147.23	1097.77

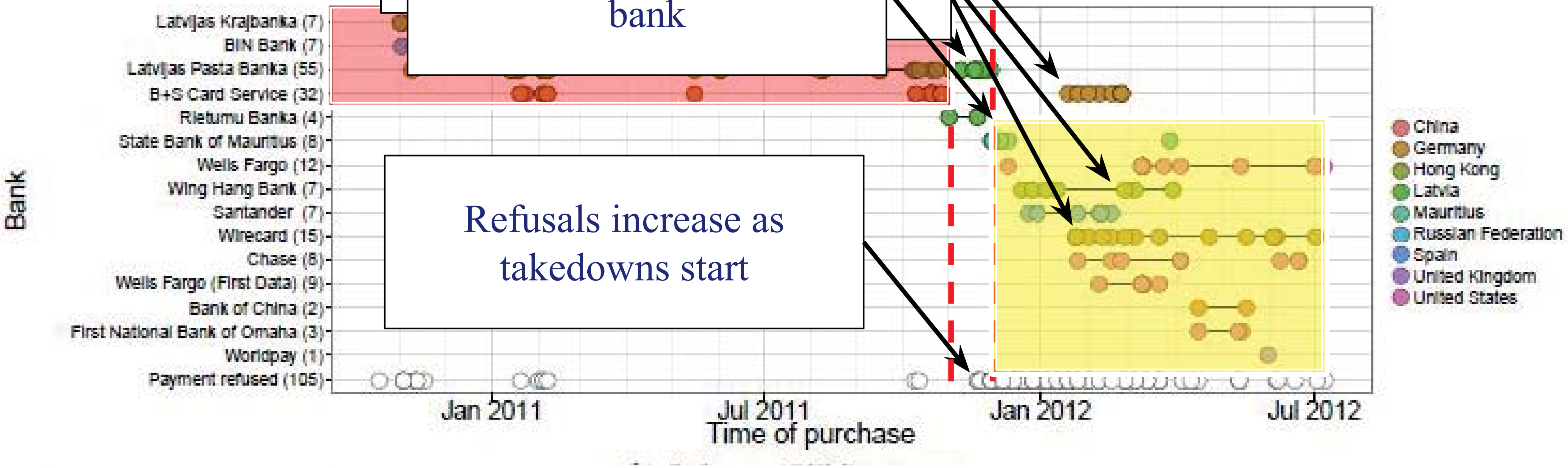
Главная | Статистика | Настройки | Промо | Переписка | Выплаты

© 2010 OemEmpire.com
All Rights Reserved

OEM software story

- Microsoft Thanksgiving surprise (Nov '11)
  - Methodically issued complaints for accounts of ***every*** major affiliate program
  - Diligent follow up:
    new pro aints (and quickly)

Scramble to find stable new bank



Refusals increase as takedowns start

Qualitative Timeline

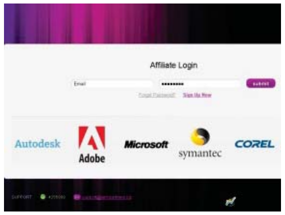
11/2011: Major software brand holder starts test purchases and merchant account complaints

11/20/2011: ATTENTION Dear advertisers, we are having problems with the bank and our accounts were suddenly frozen. We're forced to temporarily stop accepting OEM traffic.

ВНИМАНИЕ Уважаемые адверты, у нас появились внезапные проблемы с банком и нам заморозили счета. Мы вынуждены временно приостановить приём OEM трафика.

2011-11-22 10:16:38: Starting today our bank has stopped working. Due to this, we have made the decision to close our affiliate program for the duration of our search for new processing.

С сегодняшнего дня работа нашего банка прекращена(в связи с этим) о закрытии нашей ПП на время поиска нового процессинга.



1/23/2012 Remark by leading affiliate:
“The sun is setting on the OEM era”

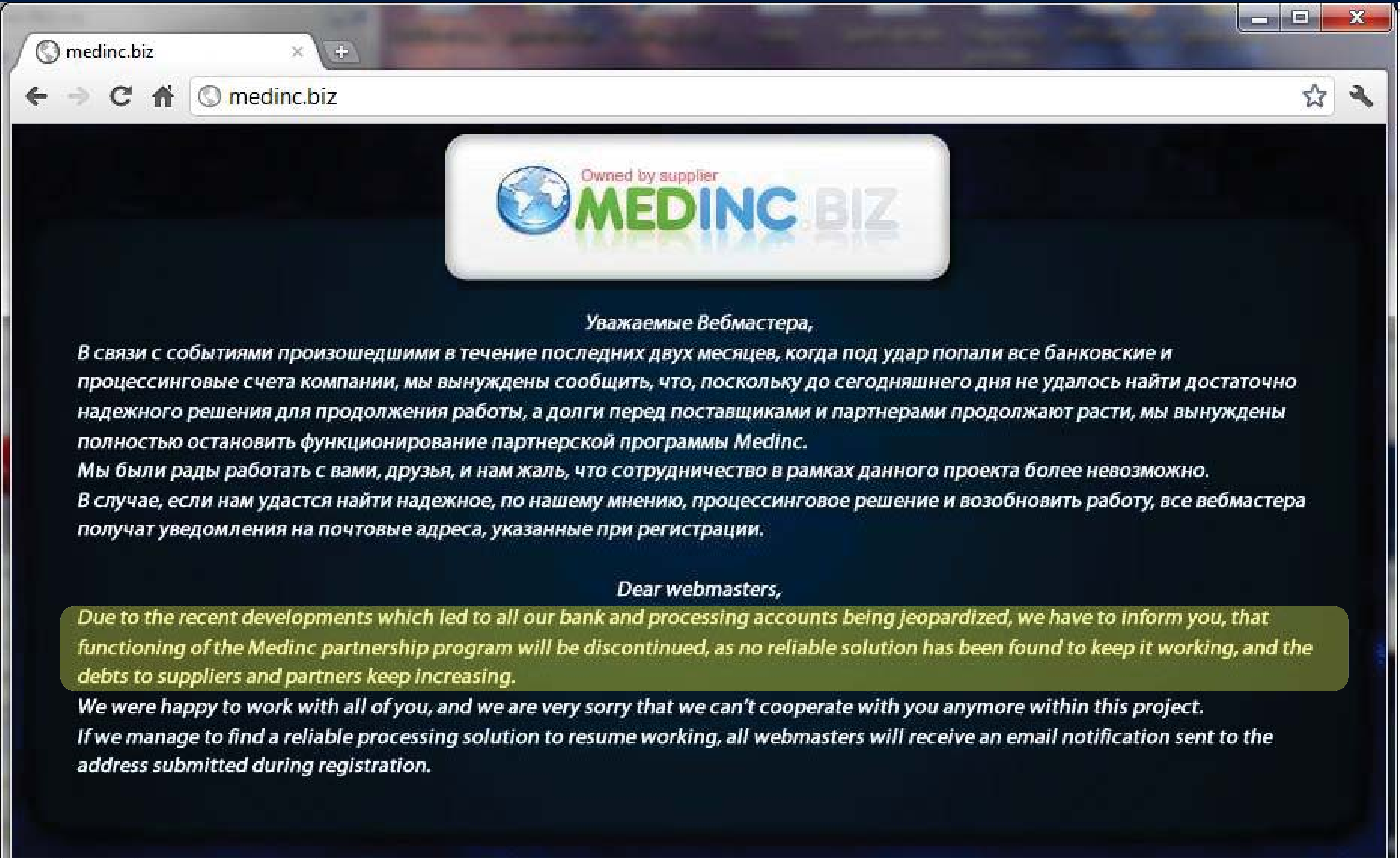
UCSDCSE
Computer Science and Engineering

OEM software story

- As of mid-late 2013
  - OEM software market was **decimated**
  - 90% of programs folded
    - Remaining programs stopped selling Microsoft software
    - MS lacked standing to issue complaint
  - Single operation effective for 18 months

- Similar story in pharma market
  - Albeit with less focus than software

Medinc.biz



Уважаемые Вебмастера,

В связи с событиями произошедшими в течение последних двух месяцев, когда под удар попали все банковские и процессинговые счета компании, мы вынуждены сообщить, что, поскольку до сегодняшнего дня не удалось найти достаточно надежного решения для продолжения работы, а долги перед поставщиками и партнерами продолжают расти, мы вынуждены полностью остановить функционирование партнерской программы Medinc.

Мы были рады работать с вами, друзья, и нам жаль, что сотрудничество в рамках данного проекта более невозможно.

В случае, если нам удастся найти надежное, по нашему мнению, процессинговое решение и возобновить работу, все вебмастера получат уведомления на почтовые адреса, указанные при регистрации.

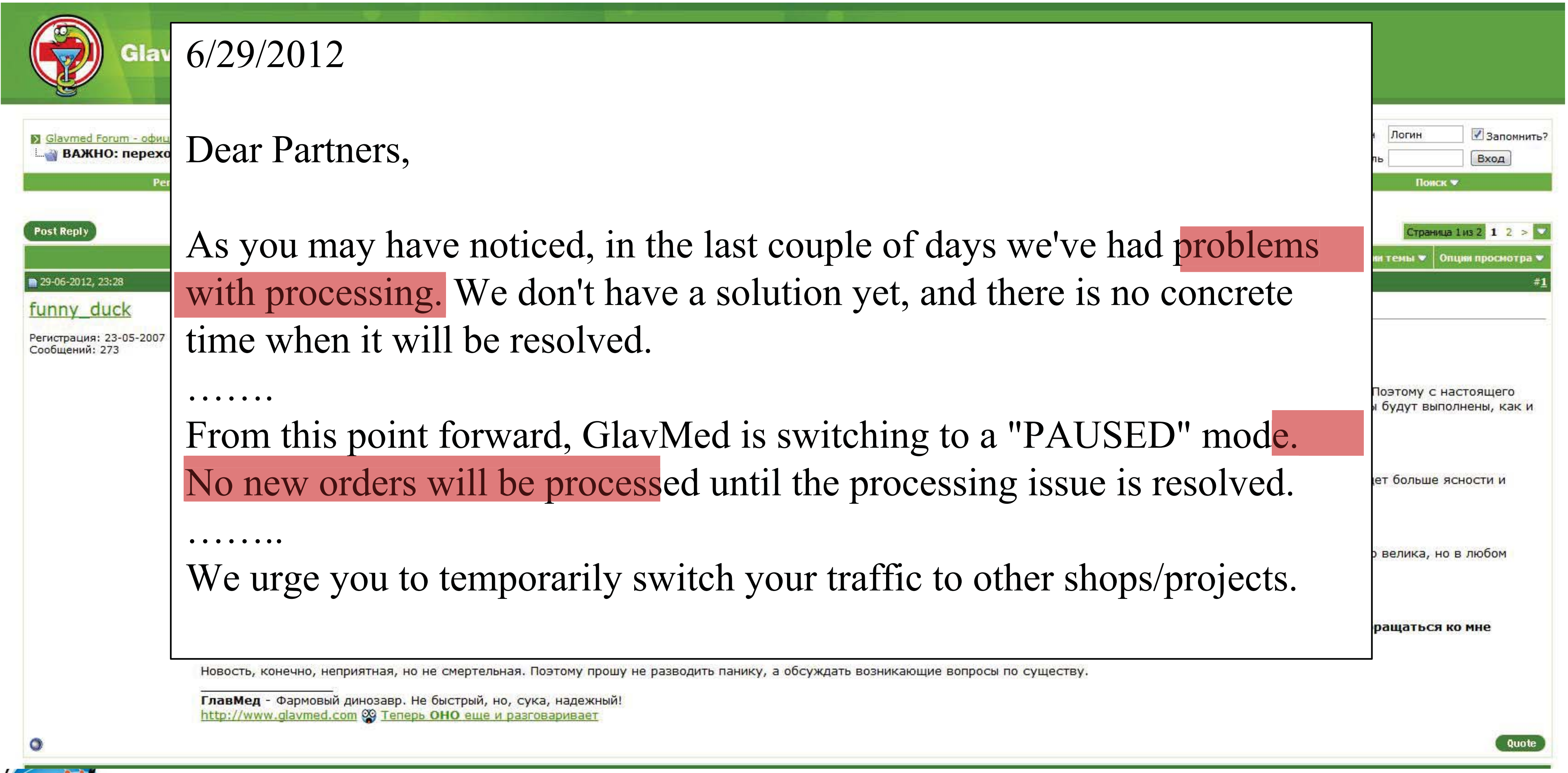
Dear webmasters,

Due to the recent developments which led to all our bank and processing accounts being jeopardized, we have to inform you, that functioning of the Medinc partnership program will be discontinued, as no reliable solution has been found to keep it working, and the debts to suppliers and partners keep increasing.

We were happy to work with all of you, and we are very sorry that we can't cooperate with you anymore within this project.

If we manage to find a reliable processing solution to resume working, all webmasters will receive an email notification sent to the address submitted during registration.

Glavmed



6/29/2012

Dear Partners,

As you may have noticed, in the last couple of days we've had problems with processing. We don't have a solution yet, and there is no concrete time when it will be resolved.

…….

From this point forward, GlavMed is switching to a "PAUSED" mode. No new orders will be processed until the processing issue is resolved.

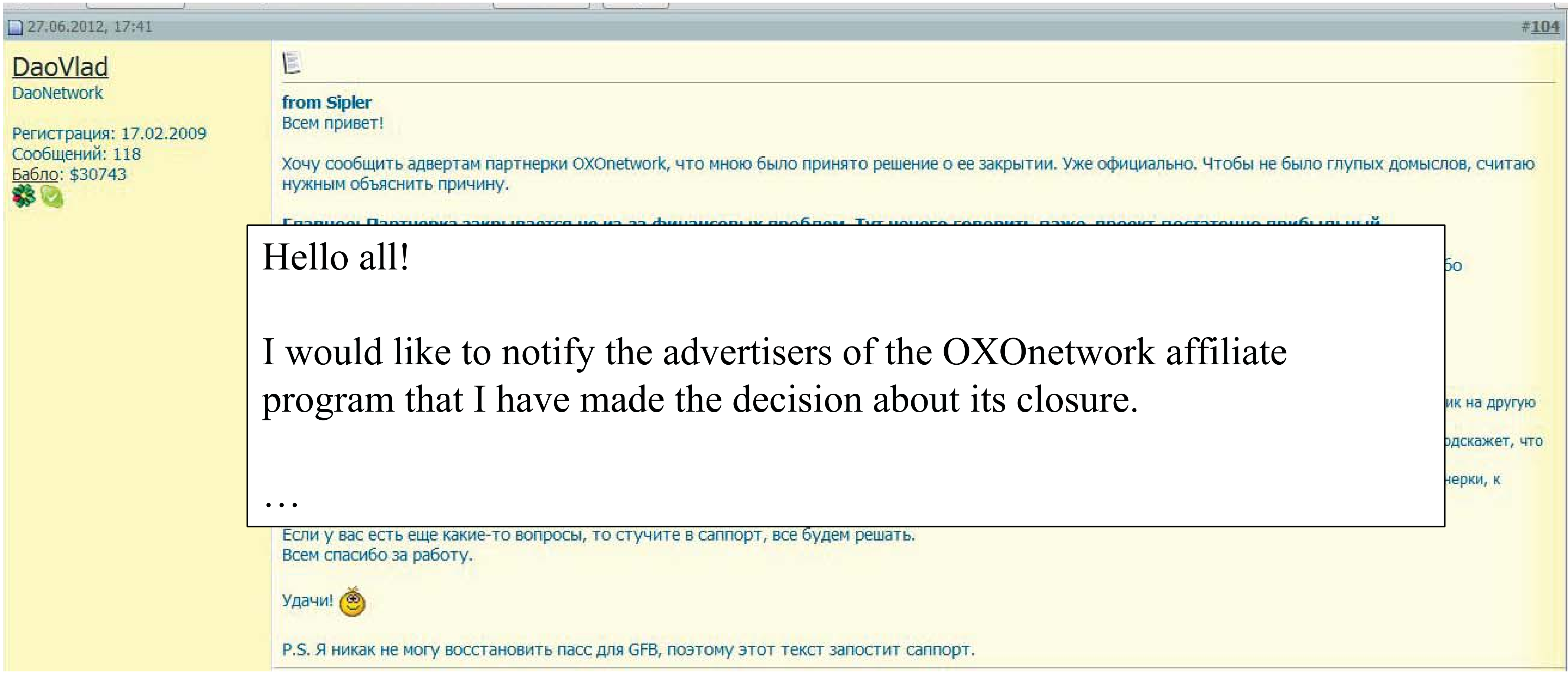
……..

We urge you to temporarily switch your traffic to other shops/projects.

Новость, конечно, неприятная, но не смертельная. Поэтому прошу не разводить панику, а обсуждать возникающие вопросы по существу.

ГлавМед - Фармовый динозавр. Не быстрый, но, сука, надежный!
http://www.glavmed.com Теперь **ОНО** еще и разговаривает

OxoPharm



27.06.2012, 17:41 #104

DaoVlad
DaoNetwork

Регистрация: 17.02.2009
Сообщений: 118
Бабло: $30743

from Sipler
Всем привет!

Хочу сообщить адвертам партнерки OXOnetwork, что мною было принято решение о ее закрытии. Уже официально. Чтобы не было глупых домыслов, считаю нужным объяснить причину.

Главное: Партнерка закрывается не из-за финансовых проблем. Тут нечего говорить даже, проект достаточно прибыльный

бо

ик на другую

одскажет, что

нерки, к

Если у вас есть еще какие-то вопросы, то стучите в саппорт, все будем решать.
Всем спасибо за работу.

Удачи!

P.S. Я никак не могу восстановить пасс для GFB, поэтому этот текст запостит саппорт.

Hello all!

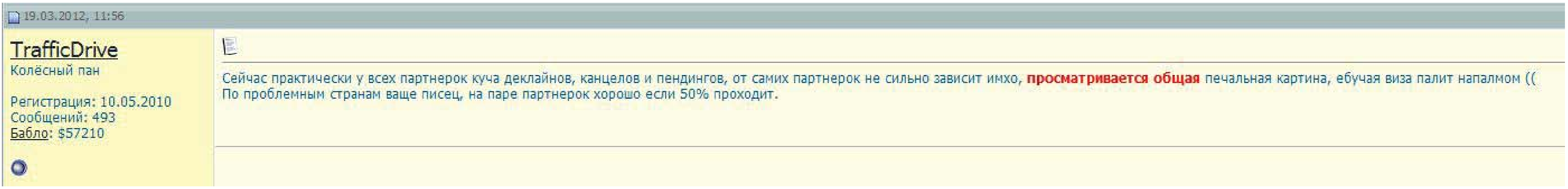
I would like to notify the advertisers of the OXOnetwork affiliate program that I have made the decision about its closure.

…

Cashadmin

- To all Cashadmin affiliates, ….
RX industry is under attack from all sides. Recently, we have lost our credit card processing abilities several times, and it has come to the point where we are losing more money processing orders than we are getting from the orders themselves. The industry has become impossible to manage and maintain. Cashadmin has closed its sites…

Life is tough all around…



19.03.2012, 11:56

TrafficDrive
Колёсный пан

Регистрация: 10.05.2010
Сообщений: 493
Бабло: $57210

Сейчас практически у всех партнерок куча деклайнов, канцелов и пендингов, от самих партнерок не сильно зависит имхо, **просматривается общая** печальная картина, ебучая виза палит напалмом ((
По проблемным странам ваще писец, на паре партнерок хорошо если 50% проходит.

"Right now most affiliate programs have a mass of declines, cancels and pendings, and it doesn't depend much on the program imho, there is a general sad picture, fucking Visa is burning us with napalm (for problematic countries, it's totally fucked, on a couple of programs you're lucky if you get 50% through)."

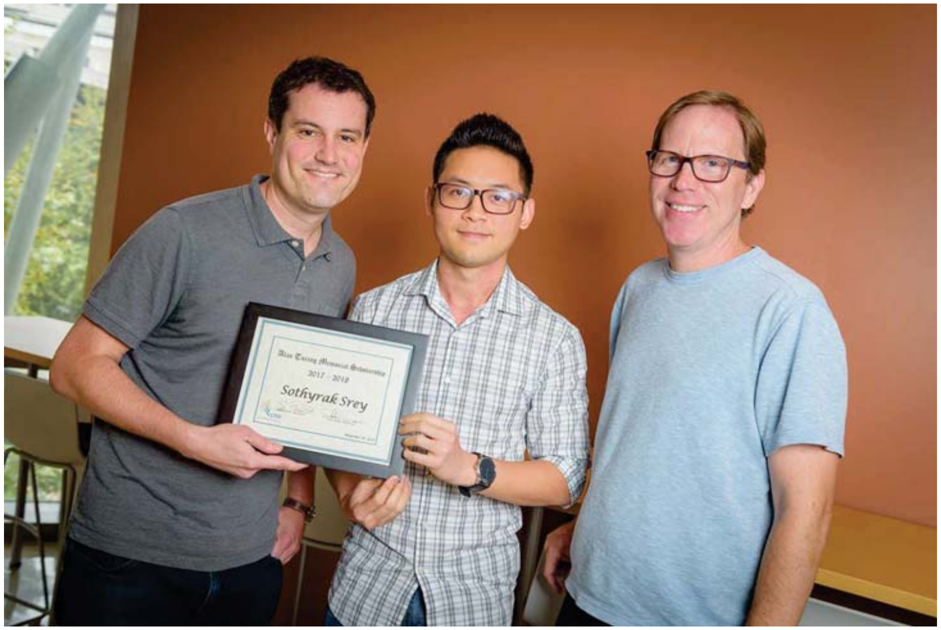
Summary

- Security is about more than just technology
  - Effective intervention requires reasoning about the **economic/social structure** of our adversaries

- There is an **achievable** research agenda here
  - Much more than I was able to talk about today
    - ***Not only spam**: malware distribution, account abuse, ad abuse, financial credentials theft, advanced fee fraud, etc*
  - **Opportunities for meaningful impact**

Alan Turing Memorial Scholarship

- Named for Alan Turing – father of computing
- Recognizes support for LGBT diversity efforts by students in CS & CE
- Working to raise $50k to endow this scholarship
- More info at: cns.ucsd.edu



2017 recipient Tee Srey

Questions?