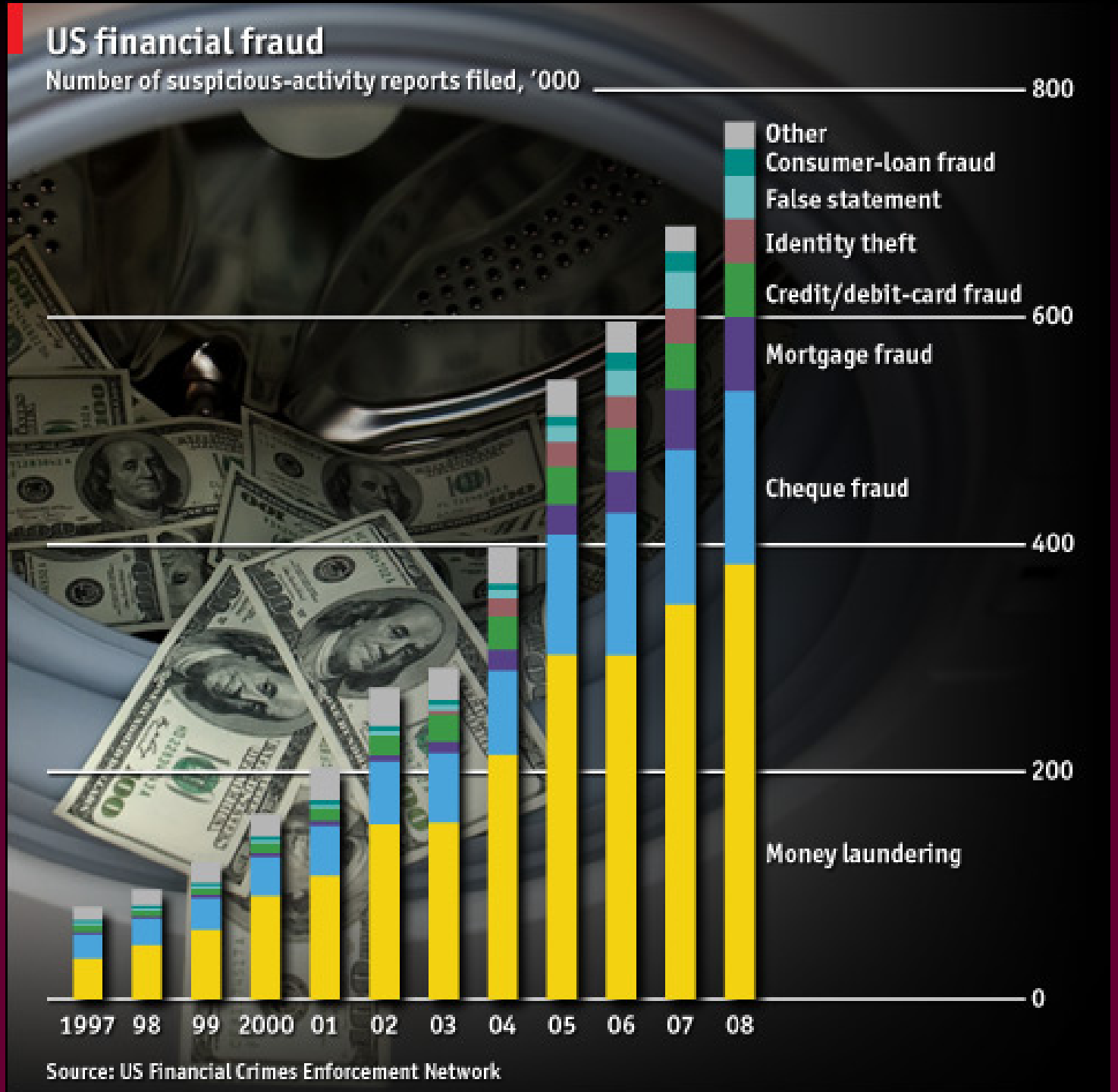
Healthcare Fraud & Fraud Control

Malcolm K. Sparrow

Professor
John F. Kennedy School of Government
Harvard University

November 2012


US financial fraud
Number of suspicious-activity reports filed, '000
800
600
400
200
0
Other
Consumer-loan fraud
False statement
Identity theft
Credit/debit-card fraud
Mortgage fraud
Cheque fraud
Money laundering
1997
98
99
2000
01
02
03
04
05
06
07
08
Source: US Financial Crimes Enforcement Network

The New York Times

July 16, 2010

Doctors, Nurses Joined Medicare Scam, U.S. Says

By REUTERS

Filed at 2:33 p.m. ET

MIAMI (Reuters) - U.S. authorities charged 94 doctors, nurses and clinic owners with scheming to defraud the taxpayer-funded Medicare program out of $251 million, Attorney General Eric Holder said on Friday.

He said 36 defendants had been arrested so far in five cities in "the largest federal healthcare fraud take-down in our nation's history."

The suspects submitted false claims for equipment and services that were not medically necessary and in many cases not actually provided, Holder said. The claims were filed through the Medicare program that provides healthcare to elderly and disabled Americans.

The Economist

Medicare fraud

Whack-a-mole

False health-care claims are huge—and spreading

Aug 12th 2010 | MIAMI

"THE largest federal health-care fraud takedown in our nation's history", was how Eric Holder, the attorney-general, described it. On July 16th authorities in five cities charged 94 people with a $251m plot to defraud the federal agency that manages health-care programmes for the poor and elderly. It was only the latest indictment in what has become a massive black hole in government spending.

The Centres for Medicare and Medicaid Services lose more than $60 billion a year to scam artists, according to the non-profit Coalition Against Insurance Fraud. About a third of the money involved in all prosecuted fraud cases is being siphoned off in south Florida, where federal agents—having missed it at first—have recently woken up. Organised-crime experts from the FBI are now involved, and judges are starting to hand down heavy sentences: in one recent case, 30 years in jail.

Typically, a "care-provider" will bill Medicare for non-existent or unnecessary services. These seem to follow fashions. First it was HIV/AIDS medicines and therapy; then medical equipment, from wheelchairs to neck and knee braces. Fraudsters have also targeted home health care, physical and occupational therapy and, most recently, mental-health services.

The Washington Times

Monday, November 30, 2009

Medicare fraudsters rake in billions

Jerry Seper and Chuck Neubauer THE WASHINGTON TIMES

Medicare fraud is a multibillion-dollar business preying on an ever-increasing number of retiring baby boomers who often are being charged for medical treatments and products they don't need and for services they don't receive.

The health care reform legislation pending in Congress -- and under debate in the Senate -- relies on reining in these fraudulent schemes to help finance coverage for the uninsured. But analysts in and out of government question whether those savings will ever be found.

Despite bolstered efforts by federal, state and local law enforcement authorities to crack down on fraudsters, abuse continues to grow.

Mail Online

The threat of the 'fake fishermen': How BP may be paying out millions in oil spill compensation to fraudsters

By Mail Foreign Service
Last updated at 11:55 AM on 12th August 2010

Cheating those who are really at risk: A genuine crab fishermen throws a trap into the waters off Louisiana earlier this month. Fears are rising that 'fake fishermen' are taking compensation meant those genuinely affected, like this man

BP could be paying millions in compensation to 'fake fishermen', it has been revealed.

IRS: EITC-based Tax-refund fraud

- Effect of Electronic Filing/Refund Anticipation Loans (1988…)

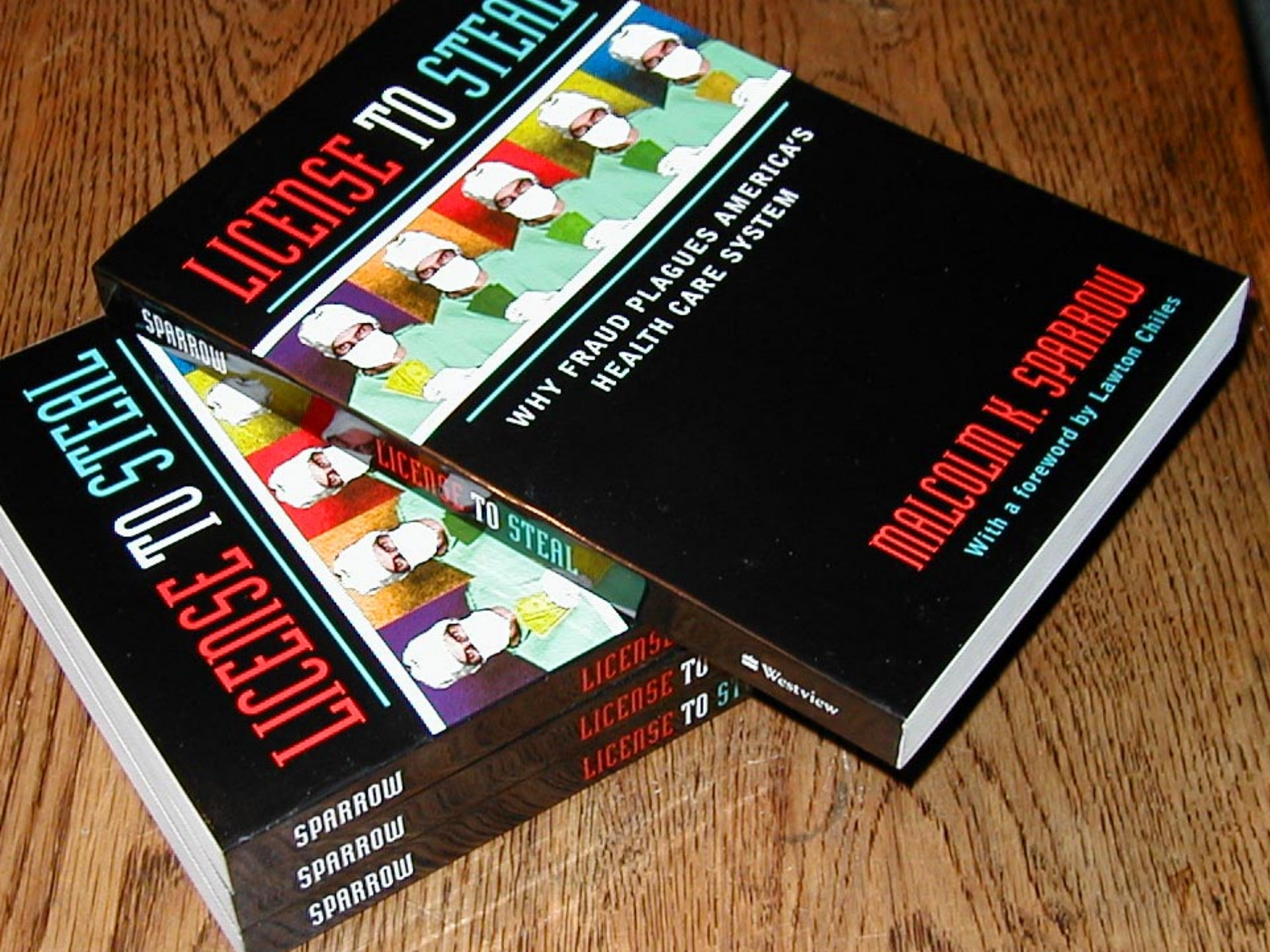
  Easy Money, Fast

- Schemes Detected:

  $7.5 million in 1989
  $ 67 million in 1992
  $ 136 million in 1993
  $ 160 million in 1994

- April 1993, NBC Dateline.

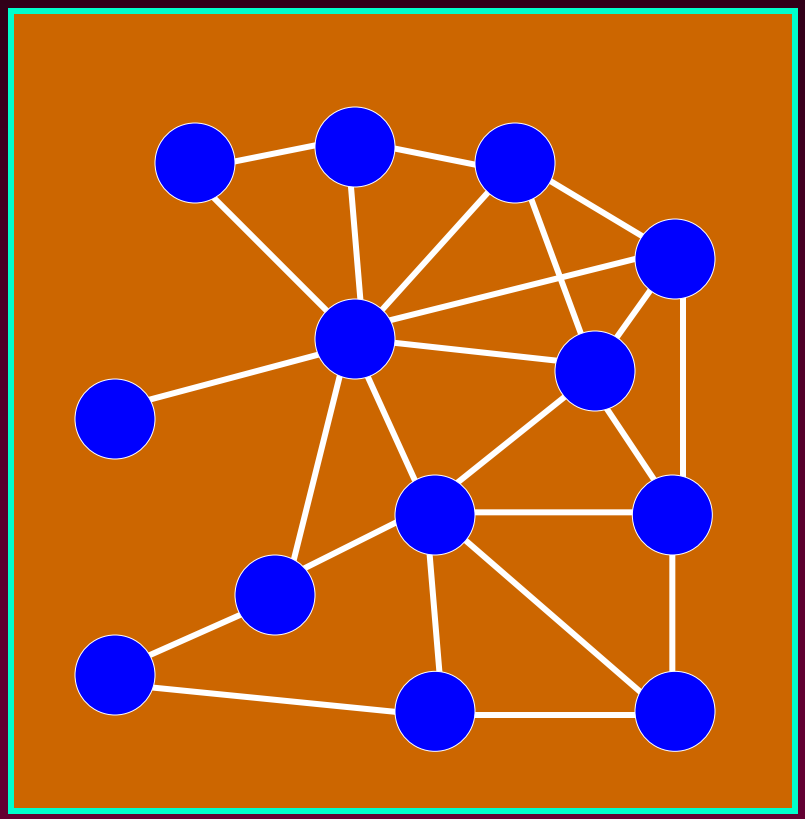
- Measurement program instituted in 1994: indicates 38.8% of EITC claims inflated or unmerited.
- 26.1% of EITC budget ($15 billion) going into wrong hands. So loss rate approximately $4 billion.
- More than $3 billion due to outright criminal fraud.
- Detection rate: 4%


LICENSE TO STEAL
WHY FRAUD PLAGUES AMERICA'S HEALTH CARE SYSTEM
MALCOLM K. SPARROW
With a foreword by Lawton Chiles
Westview
SPARROW
SPARROW
SPARROW

Ring-level Fraud:

Medicare Example: BC/BS Florida

Example - Network Algorithm

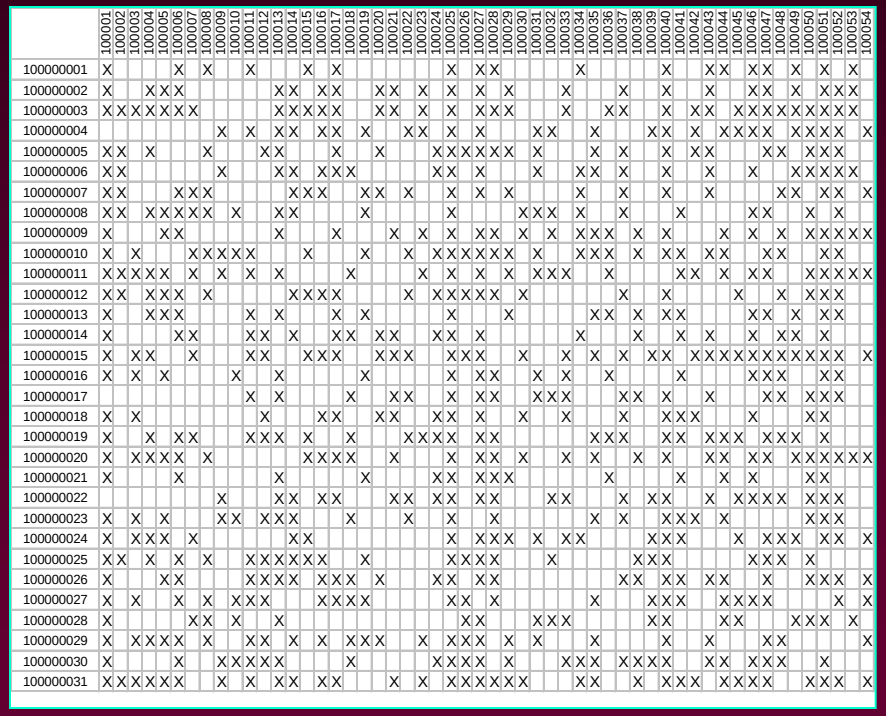


Network Concentration Algorithm

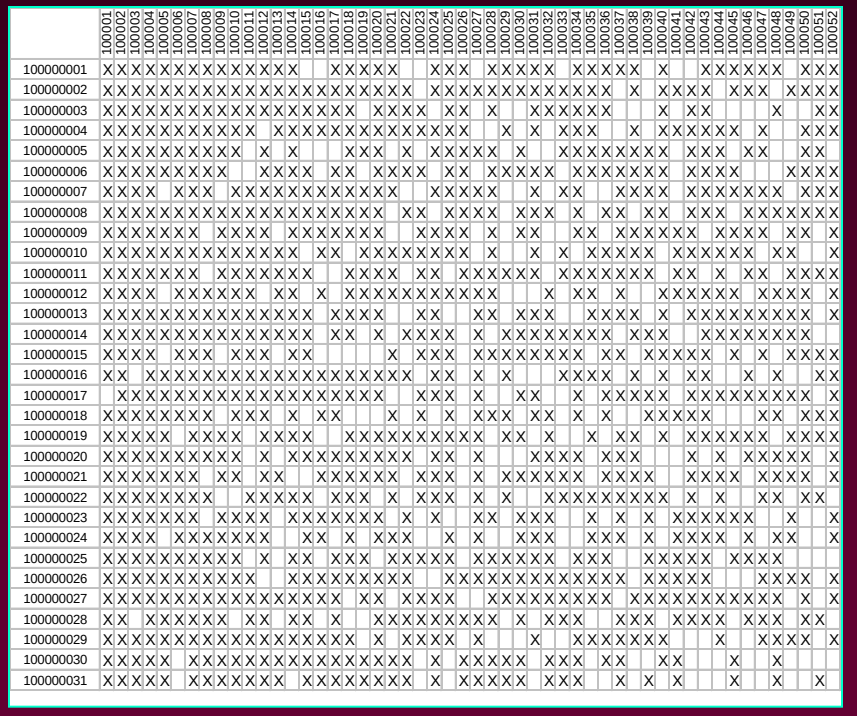
- Started with 188,403 links involving 1,381 providers and 37,911 beneficiaries
- Applied the algorithm in an iterative fashion to produce networks with increasing density of connections
- Ultimately reached level 47 with 10,564 links involving 122 providers and 181 beneficiaries

Example - Network Algorithm

Unsorted



Sorted



Malcolm K. Sparrow

John F. Kennedy School of Government, Harvard University

Example - Network Algorithm

						Accumulated				
	Number	Total Billed	Number	Total Billed	Number	Number	Total Billed	Number	Total Billed	Number
Level	Links	Within Links	Providers	for Providers	Beneficiaries	Links	Within Links	Providers	for Providers	Beneficiaries
47	10,564	58,460,988	122	326,329,100	181	10,564	58,460,988	122	326,329,100	181
46	6,897	35,058,648	43	52,141,281	109	17,461	93,519,636	165	378,470,381	290
45	1,692	8,626,792	10	9,563,546	28	19,153	102,146,428	175	388,033,927	318
44	2,402	12,119,297	13	11,354,678	42	21,555	114,265,725	188	399,388,605	360
43	1,329	6,353,708	7	5,589,966	24	22,884	120,619,433	195	404,978,571	384
42	1,510	8,282,176	8	10,863,839	28	24,394	128,901,609	203	415,842,410	412
41	1,184	5,615,818	8	5,505,505	21	25,578	134,517,427	211	421,347,915	433
40	1,034	4,560,777	8	5,655,281	18	26,612	139,078,204	219	427,003,196	451
39	1,087	5,441,172	9	8,415,515	19	27,699	144,519,376	228	435,418,711	470
38	1,062	5,049,968	7	3,234,026	21	28,761	149,569,344	235	438,652,737	491
37	1,070	5,171,512	4	1,921,515	25	29,831	154,740,856	239	440,574,252	516
36	1,183	5,951,276	7	4,072,407	26	31,014	160,692,132	246	444,646,659	542
35	1,218	5,971,479	7	3,418,120	28	32,232	166,663,611	253	448,064,779	570
34	1,389	6,823,210	11	11,004,671	30	33,621	173,486,821	264	459,069,450	600
33	1,645	7,691,355	13	7,195,119	37	35,266	181,178,176	277	466,264,569	637
32	1,020	4,737,753	9	3,871,202	23	36,286	185,915,929	286	470,135,771	660
31	925	4,639,212	7	5,246,340	23	37,211	190,555,141	293	475,382,111	683
30	1,641	7,506,638	12	4,952,348	43	38,852	198,061,779	305	480,334,459	726
29	1,733	8,296,484	13	5,705,247	47	40,585	206,358,263	318	486,039,706	773
28	1,424	7,089,883	12	8,101,192	39	42,009	213,448,146	[illegible]	494,140,898	812
27	1,051	4,904,613	9	12,167,837	30	43,060	218,352,759	339	506,308,735	842
26	1,916	9,000,332	21	6,786,441	53	44,976	227,353,091	[illegible]	513,095,176	895
25	1,420	6,791,068	11	6,960,064	46	46,396	234,144,159	371	520,055,240	941
24	1,710	8,443,317	13	10,271,792	59	48,106	242,587,476	384	530,327,032	1,000
23	1,310	6,120,406	9	6,839,893	48	49,416	248,707,882	393	537,166,925	1,048
22	1,844	8,625,291	21	13,108,959	63	51,260	257,333,173	414	550,275,884	1,111
21	1,719	8,101,689	20	7,777,343	62	52,979	265,434,862	434	558,053,227	1,173
20	1,810	8,868,591	17	7,854,687	74	54,789	274,303,453	451	565,907,914	1,247
19	1,669	7,855,227	10	4,190,956	78	56,458	282,158,680	461	570,098,870	1,325
18	1,832	8,813,577	16	8,142,934	86	58,290	290,972,257	477	578,241,804	1,411
17	1,678	7,943,613	20	7,541,838	79	59,968	298,915,870	497	585,783,642	1,490
16	1,866	8,912,324	21	7,063,865	96	61,834	307,828,194	518	592,847,507	1,586
15	1,878	9,057,741	26	13,691,779	100	63,712	316,885,935	544	606,539,286	1,686

The Pathology of Fraud Control

Malcolm K. Sparrow

John F. Kennedy School of Government, Harvard University

The Nature of the Beast

"Fraud control is a miserable business."

[License to Steal: Why Fraud Plagues America's Health Care System 1st Edition (1996); Chapter 1; 1st sentence!]

The Pathology of Fraud Control

- What you see is never the problem
  - it's the invisible piece that counts
- Available performance indicators are all ambiguous:
  - Is it better to detect more fraud, or less?
  - Recoveries double. Good news or bad?
- Fraud control flies in the face of productivity, efficiency, and service
  - resulting clash of cultures; conflicting values
- Fraud control is a dynamic game played against conscious, sometimes sophisticated, opponents
  - so new controls are *always* over-estimated
- Production environment naturally supports only transaction-level monitoring
  - but smarter perpetrators make all transactions look perfect

The Unfortunate Consequences…

- There's never any money for fraud control (except for a brief period following scandalous revelation about fraud losses)
- Fraud control seldom high on executives' priority lists
- Many parties prefer to leave the issue alone (everyone's happy, making money; why upset everyone by drawing attention to a problem you don't even know exists)
- Competent fraud analysts and investigators become outcasts within their own organizations, and die young

Fraud Perpetrators' Preference

Dream	*Nightmare*
A payment system which is:	
1. Fast	1. Slow
2. Transparent	2. Mysterious
3. Perfectly Predictable	3. Unpredictable
4. Completely Automated (No Risk of Human Review)	4. Persistent Risk of Human Review with External Validation Sufficient to Detect Fraud

Public Payment Systems: Recipe for disaster…

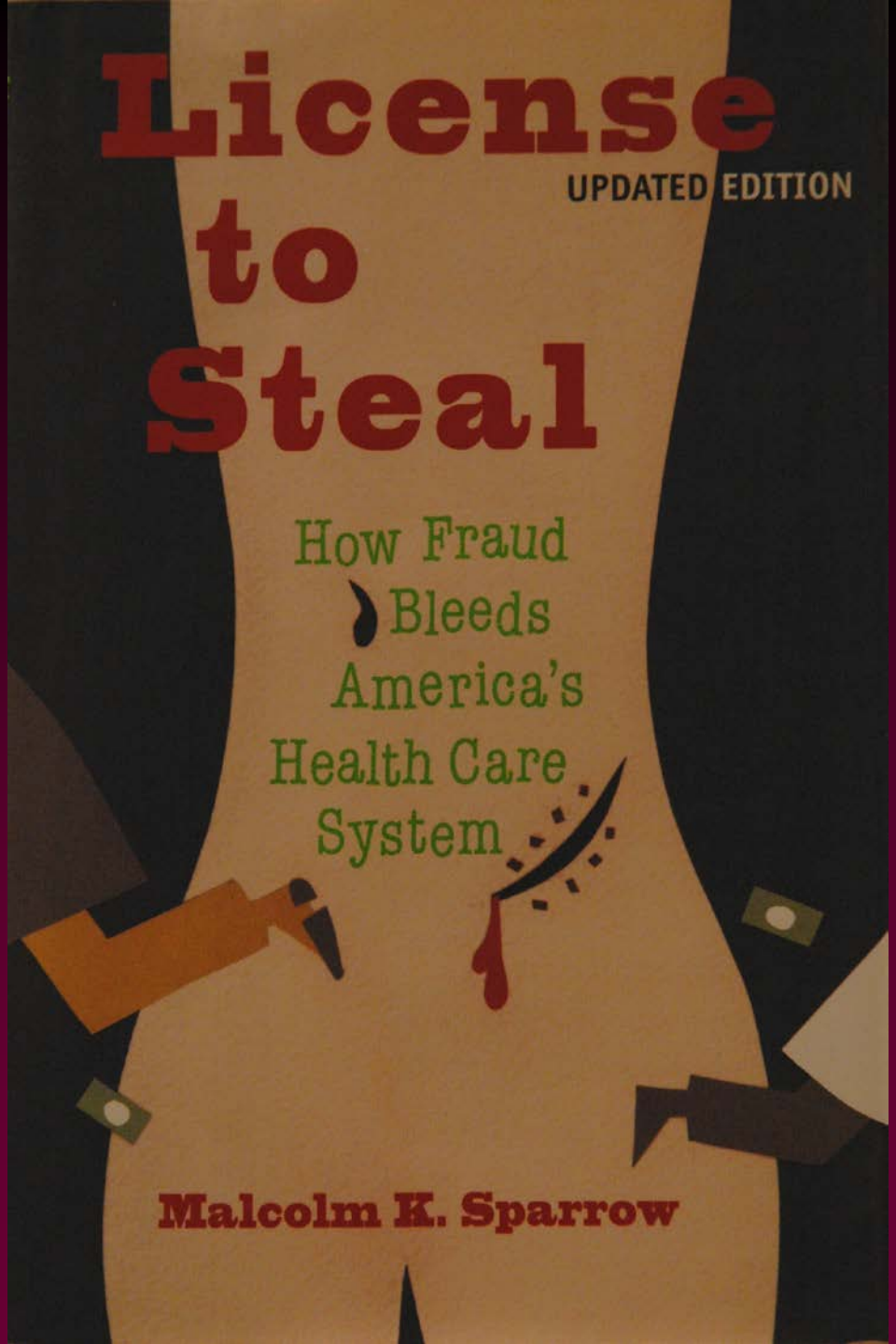
(1) Make payments electronically (welfare supports, reimbursements, health claims, tax refunds/credits, incentive payments, subsidies, etc.).
(2) Set up the system with honest claimants in mind.
(3) Allow claims & supporting documentation, to be submitted electronically.
(4) Set the administrative budget low enough that the bulk of the claims have to be paid on trust, without verification.
(5) Use computerized rule-based systems to ensure consistency and predictability in the way claims are paid.
(6) Emphasize administrative efficiency as path to cost control.

<u>To make things really dangerous</u>:

(7) Add a degree of *urgency* (e,g, stimulus funding, disaster response). Urgency tends to trump caution, and raises policymakers' perception of the "business-acceptable risk."
(8) Make it a really *valuable* program. Supporters and officials will be loath to hear any criticism of it, which will incline them to discount or downplay any reports of extensive fraud.

Three Perspectives on Fraud & Abuse (2000)

- Clinton Administration's perspective:
  - declared war on fraud and abuse in 1993
  - many legislative and other investments
  - real progress being made, error rate cut in half
- Industry perspective:
  - problem blown out of proportion
  - innocent billing errors, unavoidable
  - investigators misguided at best, jack-booted thugs……
- Consumers' perspective
  - don't believe either of the above


License to Steal
UPDATED EDITION
How Fraud Bleeds America's Health Care System
Malcolm K. Sparrow

Significant trends: 2000-2010

1) Bush Administration's pro-industry stance
2) September 11th, 2001 & its effect on federal priorities
3) Push-back against capitated managed care systems
4) Persistence, growth & centrality of Fake Billing Scams
5) Proliferation of "medically incredible" claims
6) Increased use of electronic health records
7) Obama Administration's focus on health care reform puts spotlight on cost control (odd political effects)
8) Change in official language: acknowledgment of "hundreds of billions" lost to FWA, and "low-balling" of loss estimates
9) HCF Prevention & Enforcement Action Teams (HEAT: 2009) Joint effort by DoJ/DHHS
10) Administration's commitment to substantial increases in Program Integrity spending

Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

Medicare Payments for Services After Date of Death

JUNE GIBBS BROWN
Inspector General

MARCH 2000
OEI-03-99-00200

Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

AUDIT OF SELECTED STATES' MEDICAID PAYMENTS FOR SERVICES CLAIMED TO HAVE BEEN PROVIDED TO DECEASED BENEFICIARIES

Daniel R. Levinson
Inspector General

September 2006
A-05-05-00030

Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

REVIEW OF MEDICARE PAYMENTS FOR SERVICES PROVIDED TO INCARCERATED BENEFICIARIES

APRIL 2001
A-04-00-05568

Department of Health and Human Services

OFFICE OF
INSPECTOR GENERAL

REVIEW OF MEDICARE PAYMENTS FOR SERVICES PROVIDED TO INCARCERATED BENEFICIARIES IN THE STATE OF FLORIDA

MEDICAID: A-04-01-05011 (KELLY RUBIN)

JANET REHNQUIST
Inspector General

OCTOBER 2002
A-04-02-05012

Department of Health and Human Services

OFFICE OF
INSPECTOR GENERAL

REVIEW OF MEDICAID PAYMENTS FOR OUTPATIENT SERVICES AND PRESCRIPTION DRUGS PROVIDED TO INCARCERATED RECIPIENTS IN THE STATE OF FLORIDA

JANET REHNQUIST
Inspector General

OCTOBER 2002
A-04-01-05011

Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

REVIEW OF MEDICARE PAYMENTS MADE ON BEHALF OF DEPORTED BENEFICIARIES

JANET REHNQUIST
Inspector General

MARCH 2002
A-04-01-05004

United States Senate
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
Committee on Homeland Security and Governmental Affairs
Carl Levin, Chairman
Norm Coleman, Ranking Minority Member

MEDICARE VULNERABILITIES: PAYMENTS FOR CLAIMS TIED TO DECEASED DOCTORS

STAFF REPORT

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

UNITED STATES SENATE

RELEASED IN CONJUNCTION WITH THE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS JULY 9, 2008 HEARING

Testimony before the

Permanent Subcommittee on Investigations
Committee on Homeland Security & Governmental Affairs
U.S. Senate

"Medicare Payments for Claims with Identification Numbers of Dead Doctors"

Testimony of

Robert Vito
Regional Inspector General for Evaluation and Inspections

Office of Inspector General
Department of Health and Human Services

July 9, 2008
10:30 A.M.
342 Dirksen Senate Office Building

Daniel R. Levinson,
Inspector General
Department of Health and Human Services

RECOMMENDATIONS

One piece of information that the Common Working File (CWF) uses when processing a claim is a beneficiary's date of death. We found that proper payment of a claim depends on (1) the receipt of date of death information before the claim is processed or (2) accurate system edits based on date of death information already in the CWF system. In either case, we believe that payments should not be made for services starting after a beneficiary's date of death. Therefore we recommend:

The HCFA should require Medicare contractors to conduct annual post-payment reviews to identify and recover payments for services after death

Our findings show that HCFA made substantial payments for services where the beneficiary's date of death was not yet posted at the CWF at the time the claim was processed and approved for payment. Because claims like these cannot be denied prior to payment (since the date of death is not in the CWF system), we recommend that HCFA require their contractors to conduct annual post-payment reviews to identify and recover these payments.

We also found that contractors' internal claims processing systems may be missing a significant amount of beneficiary date of death information. Therefore, HCFA should coordinate with their contractors to ensure they have the most up-to-date beneficiary date of death information before performing their post-payment reviews.

The HCFA should revise their CWF system edit to ensure that DME payments are not made for deceased beneficiaries

We found particular problems relating to DME payments for deceased beneficiaries when the CWF had date of death information at the time the claim was processed and approved

overpayments. However, prepayment screening by some States did not successfully identify the overpayments for deceased beneficiaries because the States did not use all available death information and because their payment systems had data entry, matching, and processing problems. Furthermore, although 9 of the 10 States had some form of postpayment screening, the screening did not identify all overpayments for services associated with deceased beneficiaries.

RECOMMENDATIONS

We recommend that the Centers for Medicare & Medicaid Services (CMS):

- work with States to ensure that they use all available data sources to identify deceased beneficiaries, match those data against paid claims files, and recover identified overpayments and

- encourage States to establish postpayment reviews, similar to the one we used in our 10 State-specific audits, to mitigate the effect of delays in receiving data regarding beneficiaries' dates of death.

CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

In written comments dated August 24, 2006, CMS concurred with our recommendations.

Medicare service providers.[13] Beginning in May 2008, NPIs are required to be submitted for all Medicare claims.

Based upon the Subcommittee's investigative findings and the ongoing reform of the Medicare claims review processes, the Subcommittee staff makes the following recommendations.

1. **Strengthen Procedures to Deactivate NPIs after Physician Death.** CMS should examine its procedures for identifying deceased physicians to ensure timely receipt of deceased physician data, automatic deactivation of relevant NPI numbers, and continual update of the NPI registry. CMS should develop a quality control program to ensure NPIs are deactivated within a specified period of time after receiving notice of a physician's death, such as 90 days.

2. **Initiate Regular NPI Registry and Claim Audits.** CMS should initiate periodic audits of its NPI registry to test whether NPI numbers assigned to deceased physicians have been deactivated within the specified timeframe and to test Medicare

Not using readily available deportation information in the claims processing and managed care systems puts the Medicare program at risk for making future improper payments on behalf of deported individuals. Consequently, we recommend CMS:

- use deportation information already contained in the Enrollment Data Base (EDB) to process: (1) fee-for-service claims through the Common Working File (CWF) and claims processing systems; and (2) managed care payments through the Group Health Plan (GHP) system;

---

[1]One beneficiary had both fee-for-service and managed care payments made during different time periods.

- automatically deny all Medicare fee-for-service claims and stop payments to managed care organizations for deported beneficiaries once deportation information is included in these systems;

- return the fee-for-service claims paid on behalf of the 43 deported beneficiaries to the appropriate contractors for adjudication and collection of overpayments; and

- investigate the managed care payments for the six deported beneficiaries and collect any overpayments.

…of dead patients

- What if the patients were dead?
  - Could be DME rentals, or facility charges, not terminated
  - Could be efforts to revive
  - Both can be eliminated from analysis…wait a month, and limit analysis to services that *began* after the patient was dead.
- Common in Medicaid programs. Medicare?
- OIG report "Medicare payments for Service after Date of Death" (OEI-03-99-00200)
  - $20.6 million in 1997.
  - Medicare didn't know… $12.6 million
- Two approaches:
  - Focus on "how did this claim get paid?" Process approach: implement timely/accurate filters and deny claims.
  - Focus on "how did this claim get submitted?" Crime-control approach: seize opportunity to detect phantom billers
- OIG made no inquiries regarding "how did this claim get submitted."

…and of prisoners

- OIG report (A-04-00-05568), April 2001:
  - Identified $32 million in improper Medicare FFS payments (1997-1999), w.r.t. 7,438 prisoners
- What sort of problem?
  - Option (a) Medicare shouldn't have paid
  - Option (b) phantom billings…they didn't know the beneficiaries were in prison.
- If (a): then we should improve process for screening
- If (b): how big might issue be? (BOTEC)
  - 38,600 in prison (7/19/2000) out of 40 million. (0.1%)
  - Could represent $32 billion in phantom billing
  - Process approach would help the criminals
- How to tell the difference? Find out "were the services provided?"
- Report doesn't answer that question. OIG didn't ask that question.

Assessing Fraud Risks

Assessing Fraud Risks: Which Ones are Most Dangerous?

Two Diagnostic Questions:

(1) Is the Fraud Self-Revealing?

If undetected at the time, will anyone ever know it happened?

(2) Is there a Business Opportunity in the Fraud?

Can a small number of dishonest actors do a disproportionate amount of damage?"

Watch for growth of new industry of intermediaries (handling others' transactions in bulk, make money by cheating at the margins, distributing illicit transactions broadly amongst mass of brokered transactions to evade detection.)

Examples: billing agencies and brokers (health care); bulk mail handlers (post office); "Electronic Return Originators" (IRS), etc.

BEWARE: Non-self revealing + Business Opportunity

Self-assessment guide…

Elements of a Model Fraud Control Strategy

1. Routine, Systematic Measurement
2. Resource Allocation Based on Measurement
3. Designation of Responsibility for Fraud Control
4. Problem-solving Approach to Fraud Control
5. Focus on Early Detection/Intelligence
6. Fraud-specific, Pre-payment Controls
7. Every Transaction Faces Some Risk of Review

Fraud Detection Systems

Malcolm K. Sparrow

John F. Kennedy School of Government, Harvard University

Multi-level Structure of Credit Card Fraud

Level 1: Transaction
Level 2: Card / "Plastic"
Level 3: Account
Level 4: Cardholder (Multiple Products)
Level 5: Multi-account
Extensively Collusive
"Ring" Level

Detection Tools Available in the Credit Card Industry

		Pre-Payment	Post-Payment
Level 1:	Transaction	✓	
Level 2:	Card / "Plastic"		✓
Level 3:	Account		?
Level 4:	Cardholder (Multiple Products)		
Level 5:	Multi-account Extensively Collusive "Ring" Level		

Multi-level Structure of Health Care Fraud

Level 1: Transaction
Level 2: Patient / Practitioner
Level 3: (a) Patient (b) Practitioner
Level 4: (a) Patient / Practice
(b) Policy / Practitioner
Level 5: Policy / Practice
Level 6: (a) Policy (b) Practice
Level 7: Multi-account Extensively
Collusive "Ring" Level

Detection Tools Available in the Industry

Priority for Technology Investments

		Pre-Payment	*Post-Payment*
Level 1:	Transaction	✓	
Level 2:	Patient / Provider		
Level 3(a):	Patient	✓	
Level 3(b):	Provider		✓
Level 4(a):	Patient group / Provider		
Level 4(b):	Patient / Practice (clinic)		
Level 5:	Patient group / Practice		
Level 6(a):	Defined patient group		
Level 6(b):	Practice (or clinic)		
Level 7:	Multi-party conspiracies		

Multi-Account Detection Opportunities:

- Credit card usage at hotel in Ft. Lauderdale ("point-of-compromise") with subsequent spending spree in Indonesia
- Health care: emergency treatment in Philadelphia in February, followed by visits to specific pharmacy in Washington D.C. in May, multiple patients
- Automated voice response inquiries on multiple accounts from same phone number

The Detection Game: Categories of Analysis

- Type 1: Gravitation *towards* known illegitimate behavior areas
- Type 2: Movement *away from* legitimate behavior areas
- Type 3: Unnatural *clustering* of behaviors suggestive of high level coordination
- Type 4: Things that *match* that shouldn't (inexplicable coincidence)
- Type 5: Things that *should match*, but don't.

Intelligence

Intelligence Apparatus

- *Networks of contacts* with peer organizations and law-enforcement agencies, providing early warning of any fraud trends already spotted by others
- Development of *informants* within criminal networks, who can report on emerging practices
- Interviewing *convicted fraud perpetrators*, who may be willing to describe a variety of fraud methods and who may be able to point out remaining vulnerabilities in payment systems
- *Data mining*: using a broad range of analytical tools to search for anomalous patterns. (Creative; exploration; playful……)

Intelligence Apparatus (cont.)

- *Focus groups*, providing the opportunity to pick the brains of staff, customers, and business partners about system vulnerabilities and observed patterns of suspicious behavior
- Use of *tiger teams* within the organization (whose job is to come up with creative new ways to cheat the system), as a way of testing and refining defenses
- *Scanning newspaper/magazine advertisements* describing business opportunities, or services being advertised publicly which are tangential to your business.
- *Undercover operations*, (where appropriate) to find out who's who, what's what, and what's next.

Intelligence Apparatus (cont..)

Question: Who calls the meeting at which you discuss

- what you don't know?
- what you haven't seen?
- what nearly happened?
- what happened to your neighbor?
- what you detected once, through luck?

Question: Who holds the list?

- How often are threats reassessed, monitored, tested … ?
- How do risks get added to the list?
- How often do they get removed?
- How often do risk-assessments affect resource allocations?

…goals, and methods…

"The goals are to…have student financial assistance programs removed from GAO's high-risk list by successfully addressing management deficiencies."

[The President's Management Agenda, FY 2002, Part 9, p49]

…goals, and methods…

The goals are to…have student financial assistance programs removed from GAO's high-risk list by systematically identifying and mitigating all major risks.

…goals, and methods…

The goals are to…have student financial assistance programs removed from GAO's high-risk list by constructing the systems and partnerships required to identify and mitigate risks on a continuing basis.

malcolm_sparrow@harvard.edu

http://www.hks.harvard.edu/fs/msparrow/