



Welcome

Fraud Prevention Workshop
Emerging Trends in Combating Fraud in Government





PUBLIC SECTOR PARTNERS
Bridging Needs and Solutions

Russ Hicks



Fraud Prevention Workshop

June 15, 2010

*Your system's integrity,
backed by ours.*

M Corp



Agenda & Topics

- Introductions
- Workshop Overview
- Executive Perspective
- Data Driven Fraud Framework
- Considerations In Moving Forward

Your system's integrity, backed by ours.

M Corp

MANAGING FRAUD PROACTIVELY!

CHRIS SWECKER
ATTORNEY/CONSULTANT
SWECKCHRIS@AOL.COM



TURN THE TABLES ON FRAUD NETWORKS

- AMONG YOUR GREATEST THREATS ARE FRAUD NETWORKS WORKING IN CONCERT TO CHEAT THE SYSTEM.
- “FRAUD SUPPLY CHAIN” NETWORKS ARE PERVASIVE AND VIRAL
- FAILURE TO “CONNECT THE DOTS” PLACES THE YOUR AGENCY IN A PERPETUAL REACTIVE STATE
- TO MANAGE FRAUD PROACTIVELY YOUR AGENCY MUST GO ON THE OFFENSIVE AND HUNT DOWN THE FRAUD RINGS AND NETWORKS

Which One Are You?

THE PREY



THE HUNTERS





Scope of Fraud Losses: 267 Billion

Fraud Type	Annual Losses in Billions
Health Care Fraud	60 Billion
Insurance Fraud	40 Billion
Mortgage Fraud	40 Billion
Identity Theft	47 Billion
Stimulus Grant Fraud	40 Billion
Check Fraud	40 Billion

Medicare/Medicaid Losses

- The government does not measure or estimate fraud in its programs; instead, it measures payments made "in error."
- According to Medicare's own most recent data, payments "made in error" amount to over \$10 billion annually. (Medicaid's payment errors in 2007 equaled a whopping \$32.7 billion, according to a report by the Department of Health and Human Services.)

OIG Finding re MCFU Effectiveness

- State Medicaid agency referrals accounted for 29 percent of all MFCU-reported referrals for the 3-year study period (2002-2005.)
- Previous reports examining Medicaid suspected fraud referrals found that State Medicaid agency contribution to total referrals was 35 percent in 1985 (36 States reporting) and 25 percent in 1994 (45 States reporting).
- For the 3-year period from July 2002 to June 2005, the number of referrals that an individual MFCU reported receiving from a State Medicaid agency ranged from 0 to 215 for any 1-year period and from 7 to 590 for all 3 years.

OIG Findings

- Only 3 MFCUs reported receiving over 100 referrals from State Medicaid agencies in the last year of our study: Florida (215 referrals), Arizona (192 referrals), and Texas (180 referrals).



The Threat

- Viral
- Global
- Number of Fraud Operators is Increasing
- Minimal Risk of Prosecution
- Customers/Merchants/Businesses /Agencies are One Step Behind
- Any Payment Channel That Touches the Internet is Insecure
- Opportunities are Increasing

The Strategic Challenge

Focusing on The "What" vs the "Who"

Fraud Schemes Are Unlimited

**Phantom
Payees**

**Bogus
Medical
Claims**

**Premium
Diversion**

**No
Coverage**

**Illegal
Kickbacks**

**Fake
Clinics**

**Pre-existing
Injury**

**Bogus
Lawsuits**

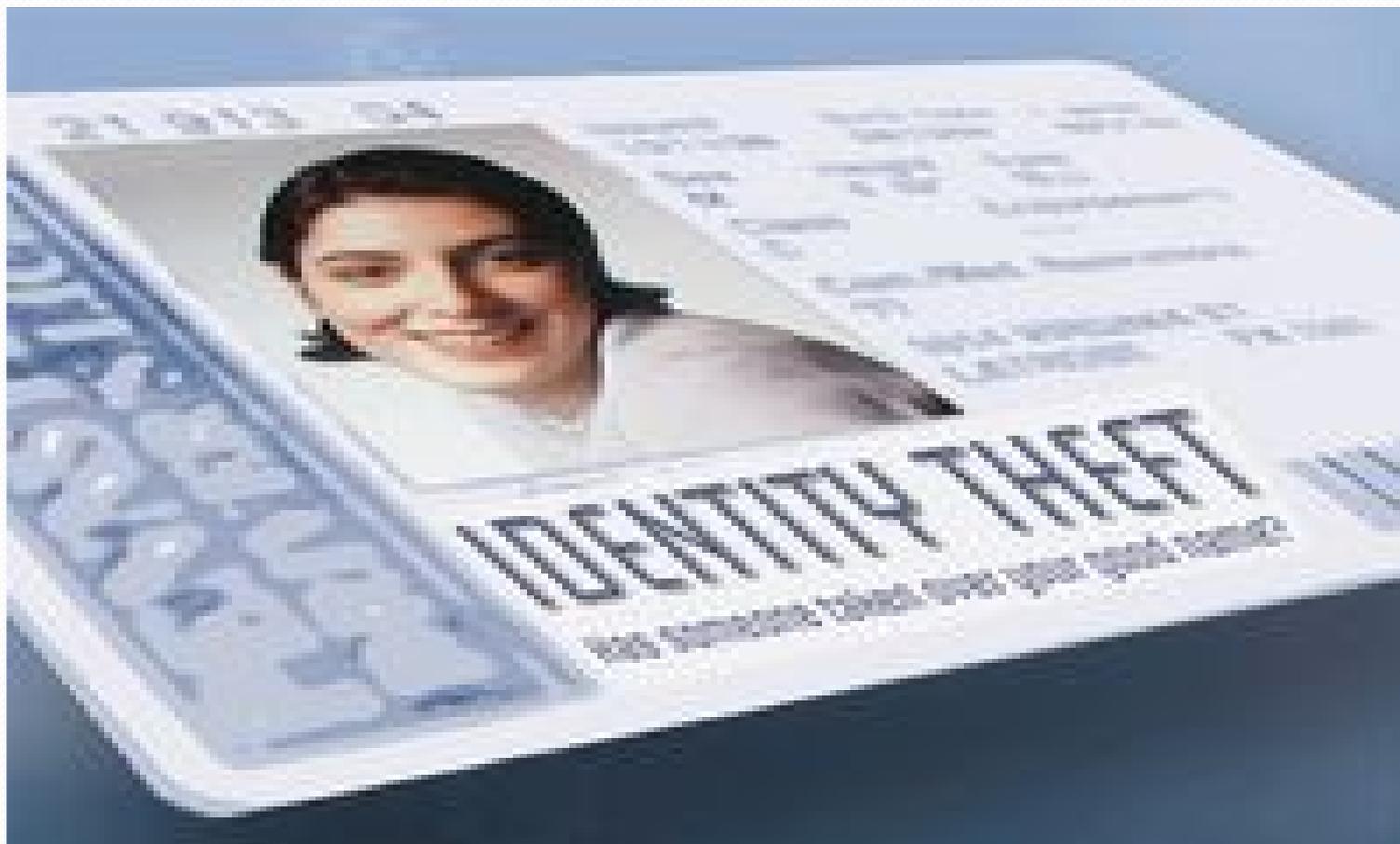
**Inflated
Injuries**

**Crooked
Lawyers**

**Double
Billing**

**Injury Off the
Job**

The Tools of Government Fraud

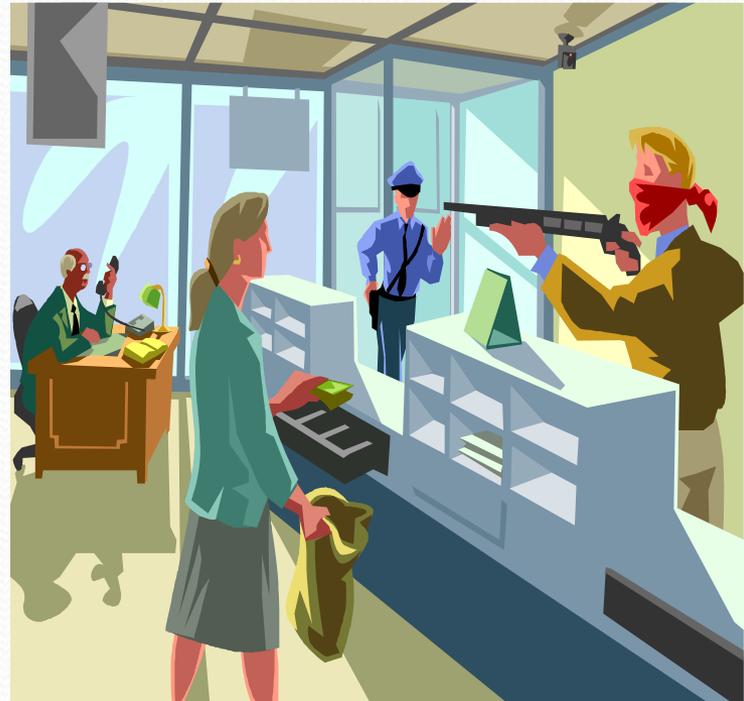


Fraud Risk Management Decision

Minimal Risk of Prosecution/Easy Money

Low Risk-High Reward

Low Reward-High Risk



STATE CATCHES FRAUD RING GETTING UNEMPLOYMENT

- With the help of a high-tech data mining staff and an investigation into phone records, the state has cracked down on a national ring of scammers collecting unemployment benefits
- Fraud investigators were tipped off to the scheme in July when several claims used the same Washington-based cell phone number.
- Investigators have identified at least 54 people who they believe have improperly collected more than \$400,000. The people live in several states, including Montana, Texas, Louisiana and Florida.

DME Fraud Out of Control

- The Department of Justice has tried to protect taxpayers from a fleecing. In South Florida, federal agents recently conducted spot checks of 1,581 firms that billed Medicare for durable medical equipment. Of these firms, 491 — nearly a third — were fictitious storefronts submitting bogus bills to the government and stealing taxpayer dollars

Dead Doctors

- In testimony last spring before a U.S. Senate subcommittee on crime, Professor John Sparrow a f Harvard fraud expert told Congress of the particularly embarrassing discovery that Medicare had made lots payments to doctors who were actually deceased and whose names had been submitted by criminals. "From 2000 to 2007, between \$60 million to \$92 million was paid for medical services or equipment that had been ordered or prescribed by dead doctors. In many cases, the doctors had been dead for more than ten years," Sparrow said.

Organized Crime Gangs are Exploiting a New Target for Illegal Profit: Medicare and Medicaid.

- Two members of a Nigerian organized crime ring are charged with defrauding Medicare of \$6 million.
- Experienced in running drug, prostitution and gambling rings, crime groups of various ethnicities and nationalities are learning it's safer and potentially more profitable to file fraudulent claims with the federal Medicare program and state-run Medicaid plans.
- "They're hitting us and hitting us hard," said Timothy Menke, head of investigations for the Office of Inspector General at the Department of Health and Human Services. "Organized crime involvement in health care fraud is widespread

The Threat

“Criminals who commit health care fraud are becoming more sophisticated and are often organized crime enterprises. They are preying on both providers and beneficiaries by illegally obtaining their provider or enrollment information and using it to submit fraudulent billings to Medicare and Medicaid”

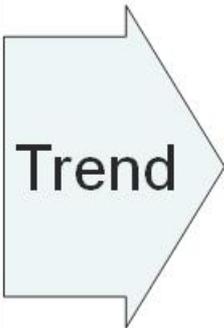
William Corr, Deputy Secretary HHS

Worrying trend...

Opportunistic individuals

- Work alone
- Single identity
- Target one organization
- Limited understanding of systems
- Little knowledge of thresholds
- May know an insider
- Focus on one product/brand
- Focus on one mode of fraud at a time
- Impatient & often greedy
- **Traditional systems and software products using scorecards and profiling alone focus on only preventing opportunistic fraud**

Trend



Professional criminals

- Work in organized gangs
- Multiple fraudulent identities
- Target multiple organizations/brands
- Detailed fraud systems knowledge
- Continually test thresholds
- Place and/or groom insiders
- Use many products/brands concurrently
- Operate multiple fraud modes & evolve continuously
- Patiently operate below the radar
- **Enhanced focus on networking fraud data will detect and prevent both opportunistic and professional/organized fraud**

Criminal Violations That Support Terrorist Financing

- Check, credit card, loan and debit fraud
- Health Care Fraud
- Cigarette Tax Fraud
- WIC Fraud
- Stolen Infant Formula
- Copyright violations
- Insurance Fraud
- Mortgage Fraud
- Internet fraud schemes
- Investment frauds
- Drugs (Spain, UK and Bali Bombers financed by crimes)
Taliban, FARC fully financed by drug cultivation and wholesale sales.



FRAUD SUPPLY CHAIN

- Data/Equipment/Knowledge Acquisition (Theft)
- Data Fencing/Equipment Sale/Knowledge Passes
- Monetization
 - This is where fraud operator's vulnerabilities begin to show
 - Data is "captured"
 - Links are made with this data
 - Money Mules Surface and act
- Proceeds Laundered

FBI Underboss Says Cyber Criminals The New Mafia

Steve Chabinsky: FBI DAD Cyber

- A determined adversary will always be able to penetrate a targeted system
- Cyber crime holds the potential to cripple businesses and services
- Serious cyber crime is becoming dominated by criminals who view themselves as businessmen...and cyber crime is their business
- These criminals work like “corporations” with extraordinary logistics.

Cyber Mules

- Mules and their handlers have done their homework—they know how agencies attempt to flag fraud, attempt make claims that go unnoticed, and often purchase cell phones in the area codes of the so that their location when verifying transfers via phone seems legitimate.
 - One and Done
 - Career
 - Premier
 - Franchisers

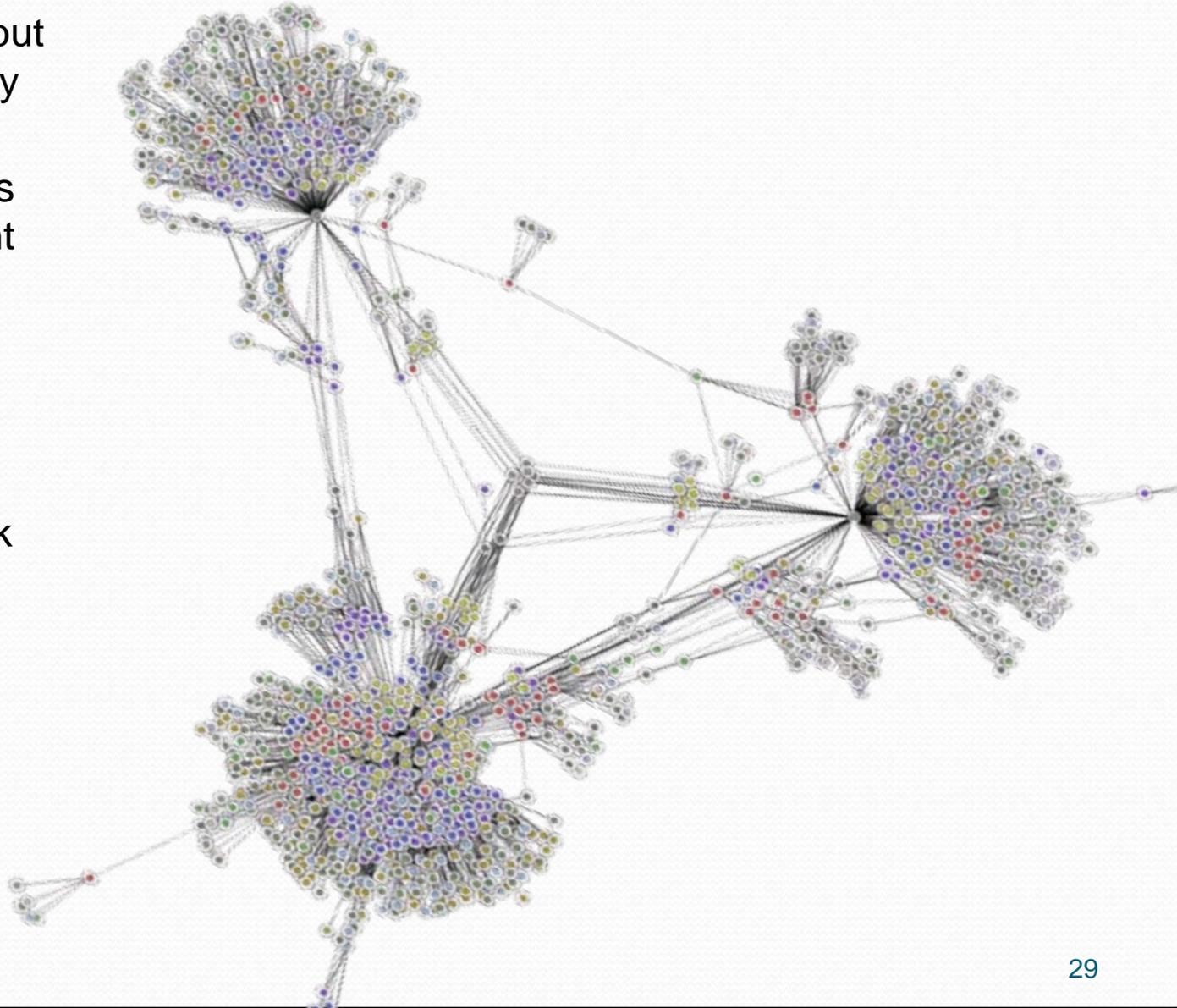
Specializations

- Coders or programmers
- Distributors or vendors
- Techies
- Hackers
- The fraudsters
- Hosters
- The cashers
- Tellers
- Money Mules
- Leaders

The Whac- a- Mole Strategy is not Enough

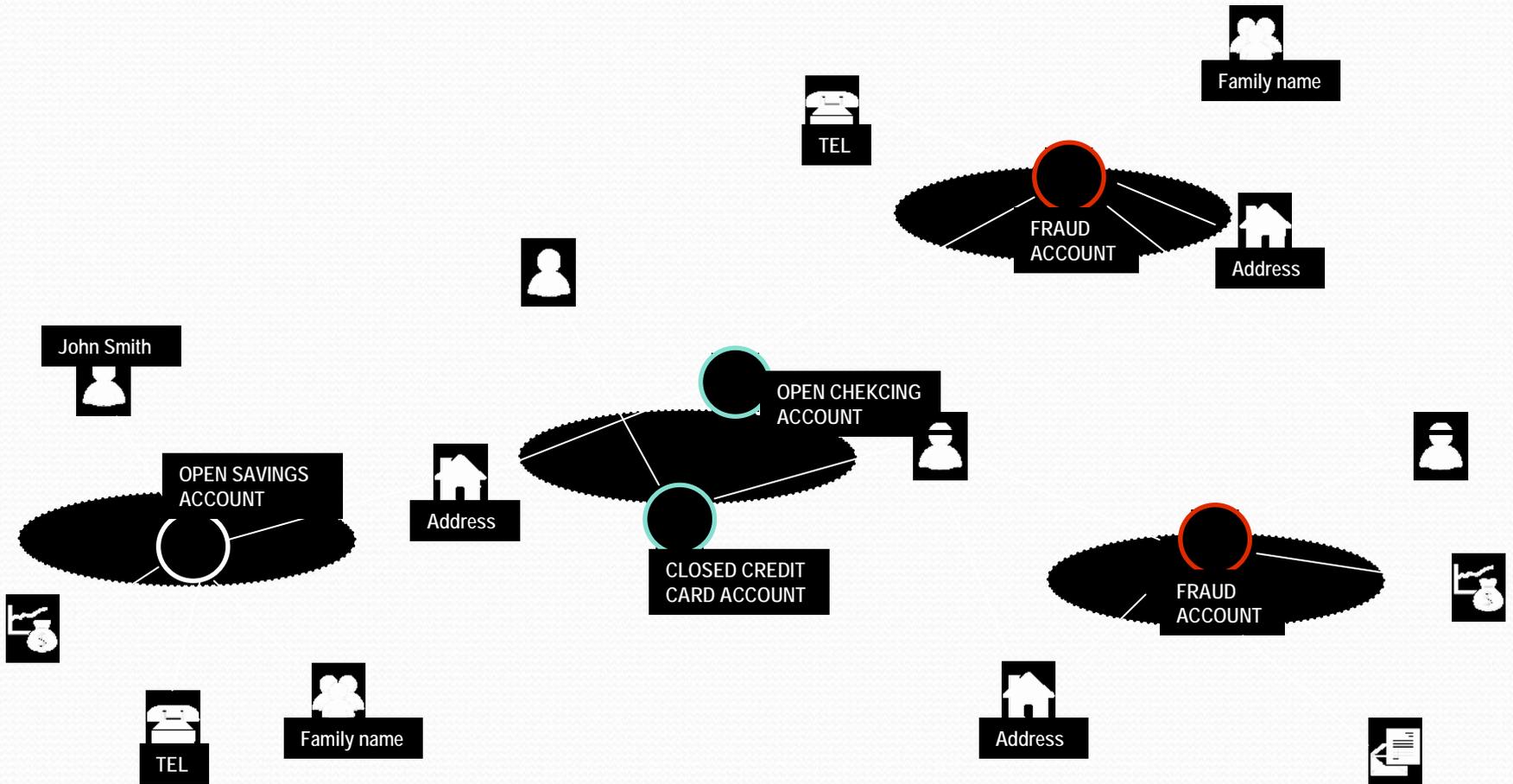


- Many user accounts but one underlying identity
- In this network there are multiple fraudsters collaborating (different identities – some common details)
- Red indicates “known fraud”
- Notice the obvious “Hubs” in this Network



Social Network of Fraud

People & Transactions Are Socially Connected



NICB Model

“It Takes a Village”

- Industry Shares Claims data
- NICB has 175 investigators and analysts dedicated to identifying insurance fraud rings and networked fraudulent activities
- They share intelligence, trends and patterns and active networks that have been identified
- “Questionable claims” referred to NICB for development of case and linking to a Fraud Ring utilizing link analysis software
- NICB says “the more data provided to analyze the better chance of making a link
- Losses reduced/deterrent introduced

Multi Agency Strategy: Going Hunting!

- Present a Deterrent/Introduce Risk to the Fraud Profession
- Join Forces to Identify the Fraud Networks
- It Takes a Network to Catch a Network
- Hunt Down the Fraud Networks
- Interrupt the Supply Chain
- Help Law enforcement Make Prosecutable cases
- Tear Down Those Walls
- The Obstacles are More Cultural Than Legal



**THE
POWER
TO KNOW[®]**

Breaking Down Fraud Silos

Integrating Detection Capability Across an Organization

Stu Bradley
Director – SAS Fraud and Financial Crimes Practice

Fraud – a Multi Industry Epidemic



According to javelin research, some **6.8 million Americans** were victimized by card fraud in 2007. They estimate losses at some **\$30.6 billion** in 2007.¹



“More people tolerate fraud and are softer about punishment”. The coalition estimates **\$80 Billion in US insurance fraud annually**.²



The National Health Care Anti-Fraud Association (NHCAA) estimates **conservatively that 3% of all health care spending—or \$68 billion—is lost** to health care fraud.³

An estimate by the FBI places the loss due to health care fraud as high **\$226 billion each year**.⁴

The **Foodstamp program's** improper payment rate is about 6 percent, costing taxpayers about \$1.7 billion annually.⁵

Almost **\$4 billion** of annual **Unemployment Insurance** benefits are improper or fraudulent.

Supplemental Security Income program pays out **\$4.6 billion** in improper and fraudulent benefits annually.

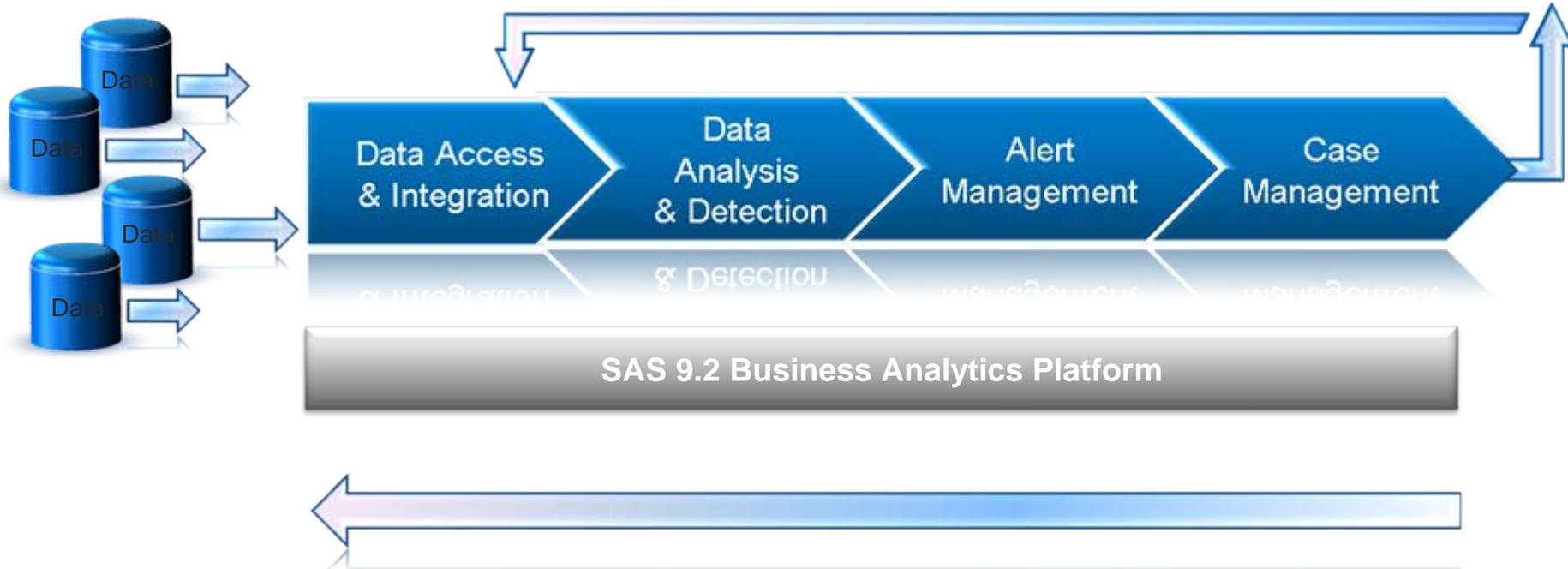


The Fraud “Perfect Storm”

Increasing Fraud - The Business Problem

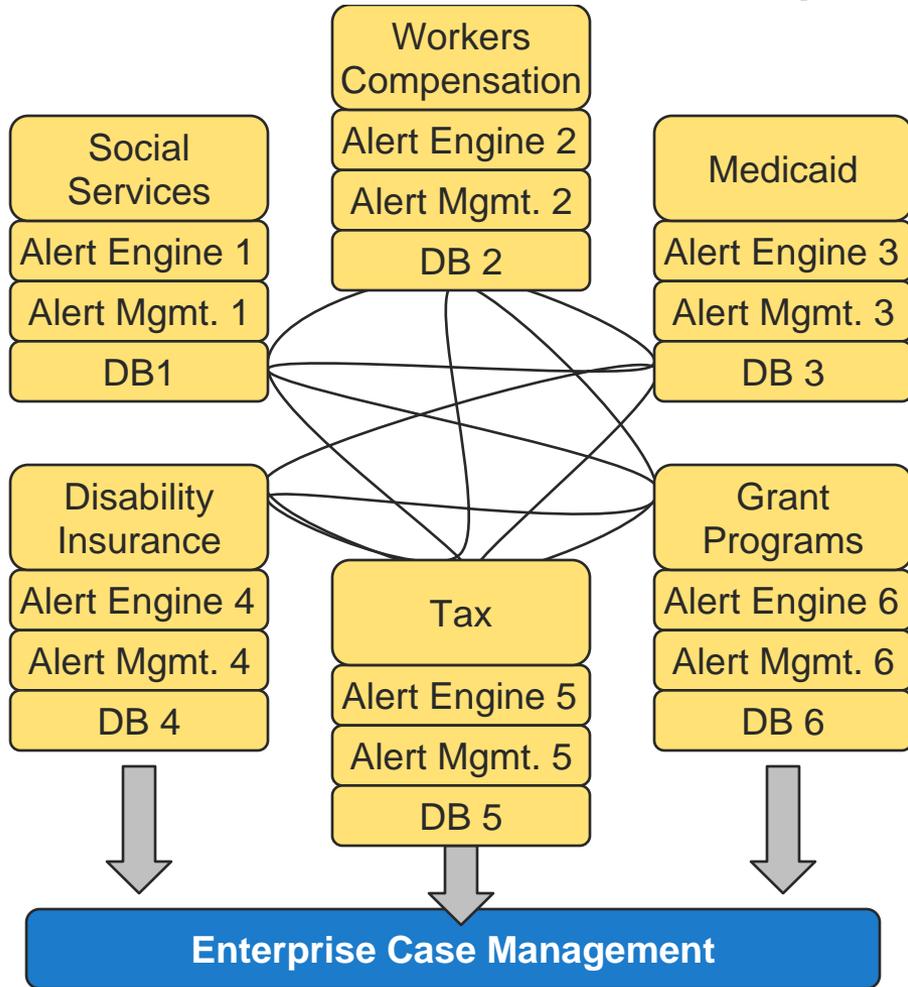
- Fraudsters
 - Far more sophisticated – organized, patient, share rules
 - Engage insiders to understand detection environment
 - Hit multiple channels and industries at the same time
 - Continuously evolve fraud strategies
 - High velocity of attacks – disappear after 2-3 transactions
- Current Fraud Systems
 - Silo'd by agency / lines of business – No sharing of data
 - Act only on transactions or entities
 - Rules and predictive models have limitations
 - No real proactive steps taken to combat cross channel fraud
 - Evidence insufficient to act upon

Trend in Fraud Detection – Upstream Integration

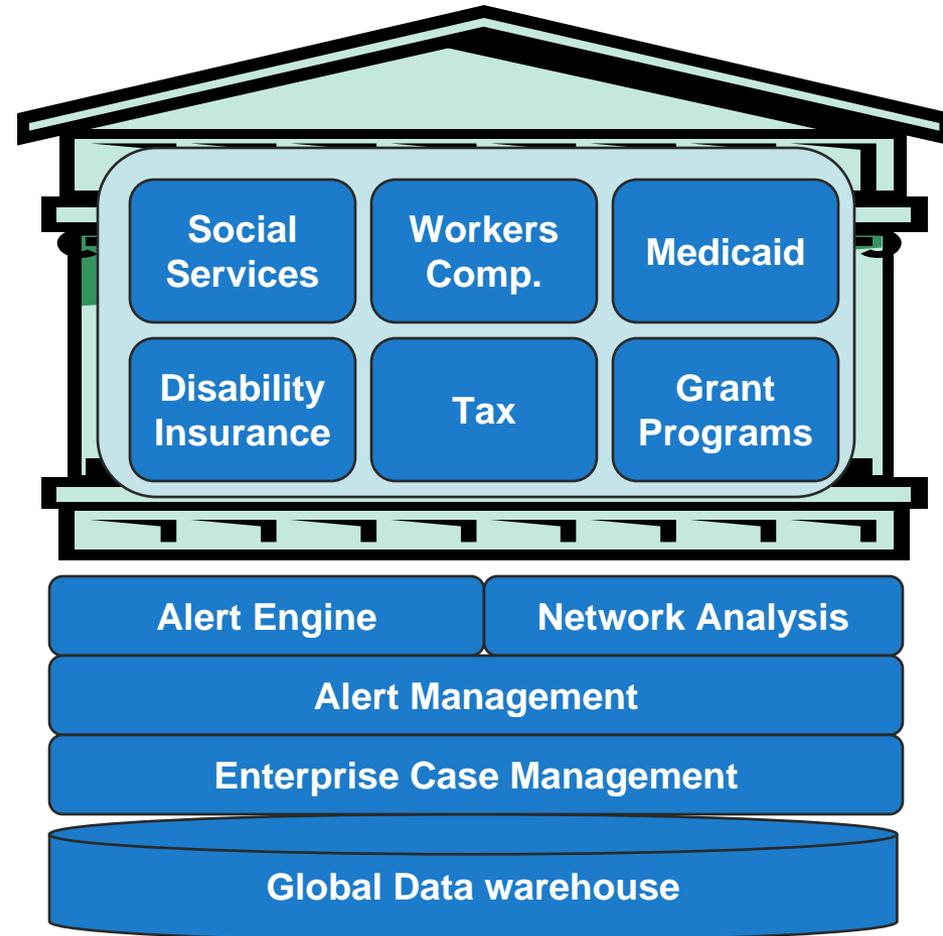


Trend is moving integration of data and analytics upstream in the fraud management process

Government Landscape



Enterprise Fraud Vision

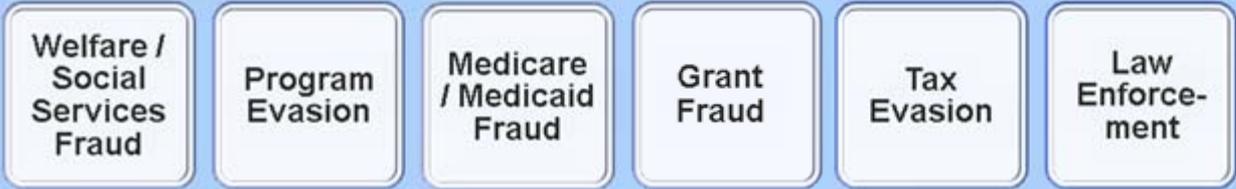


Enterprise Fraud Platform

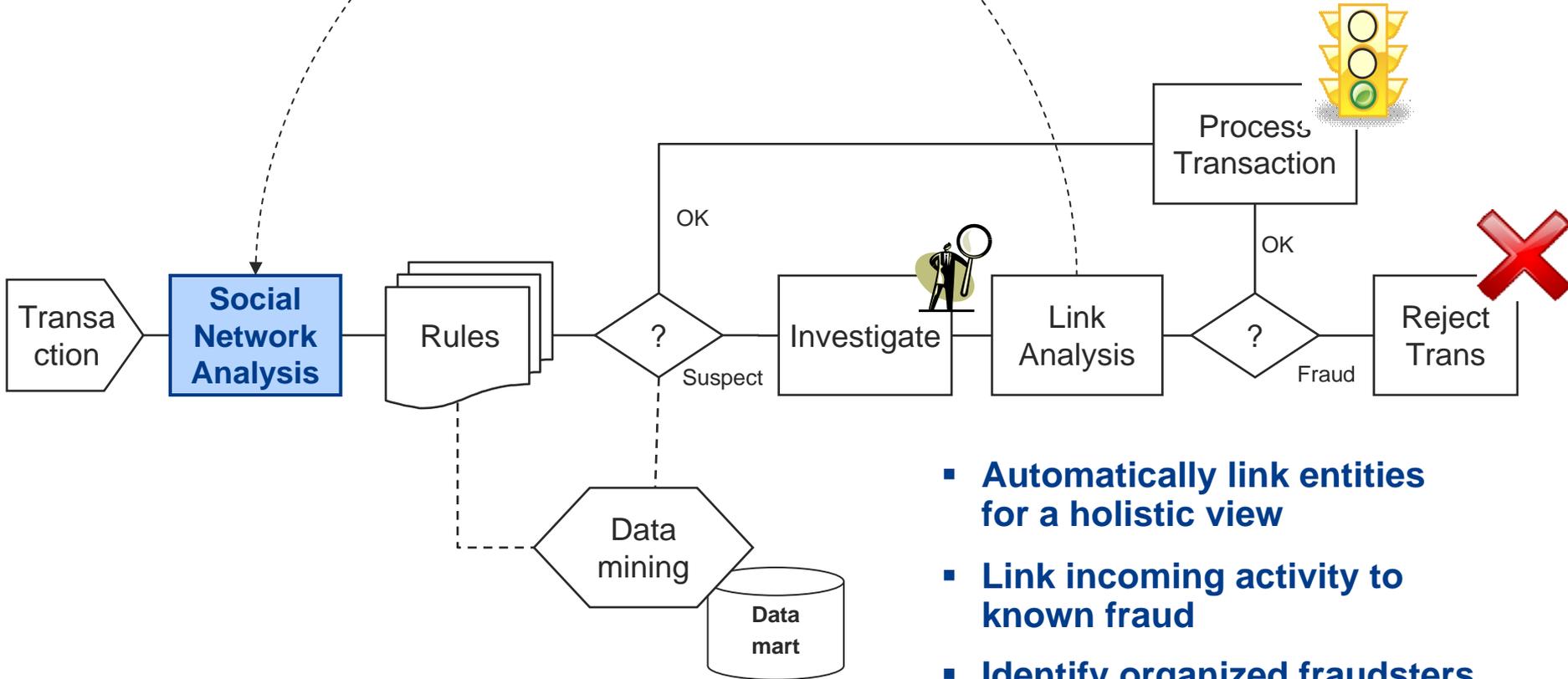
9.2 Business Analytics Framework

SAS Fraud Framework Core Components

Government Solutions (sample)



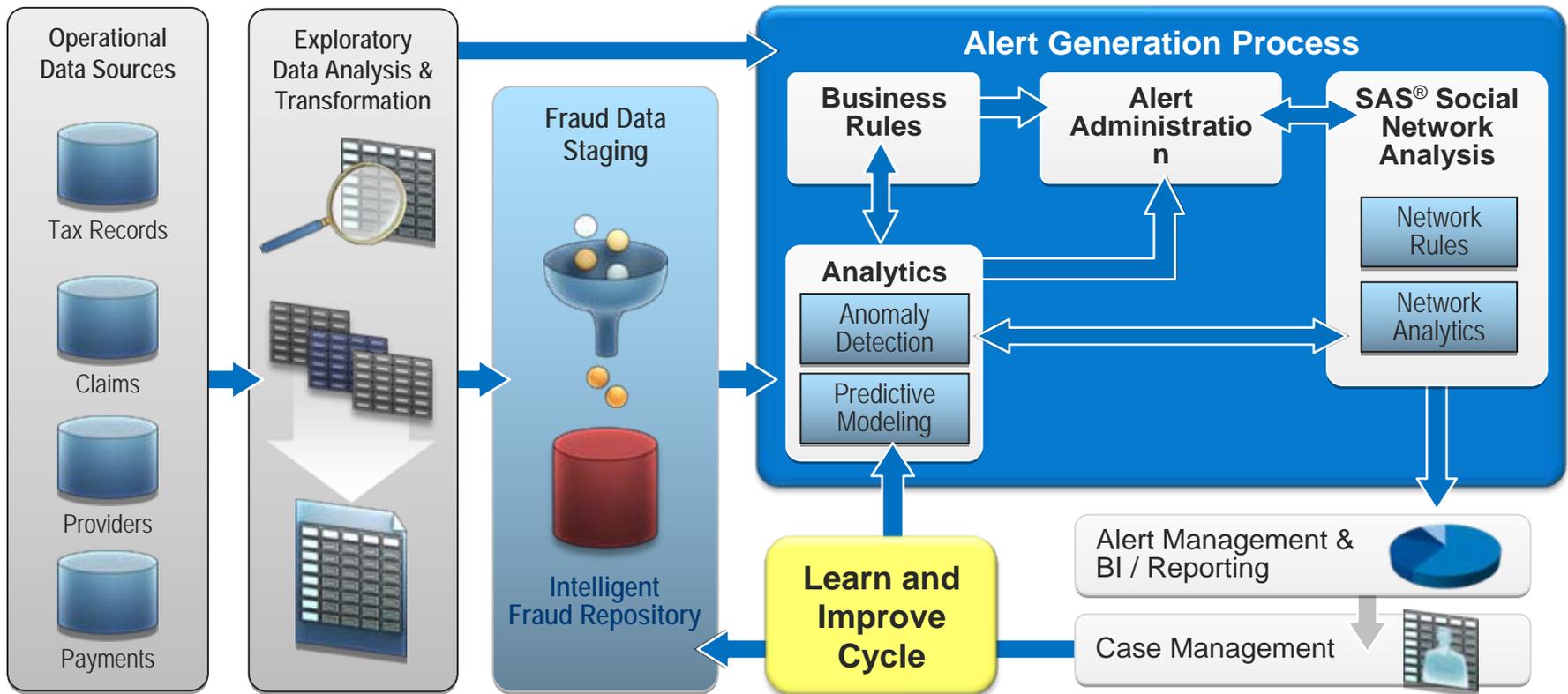
Approach needed for combating sophisticated fraud



- **Automatically link entities for a holistic view**
- **Link incoming activity to known fraud**
- **Identify organized fraudsters maintaining activity below thresholds**

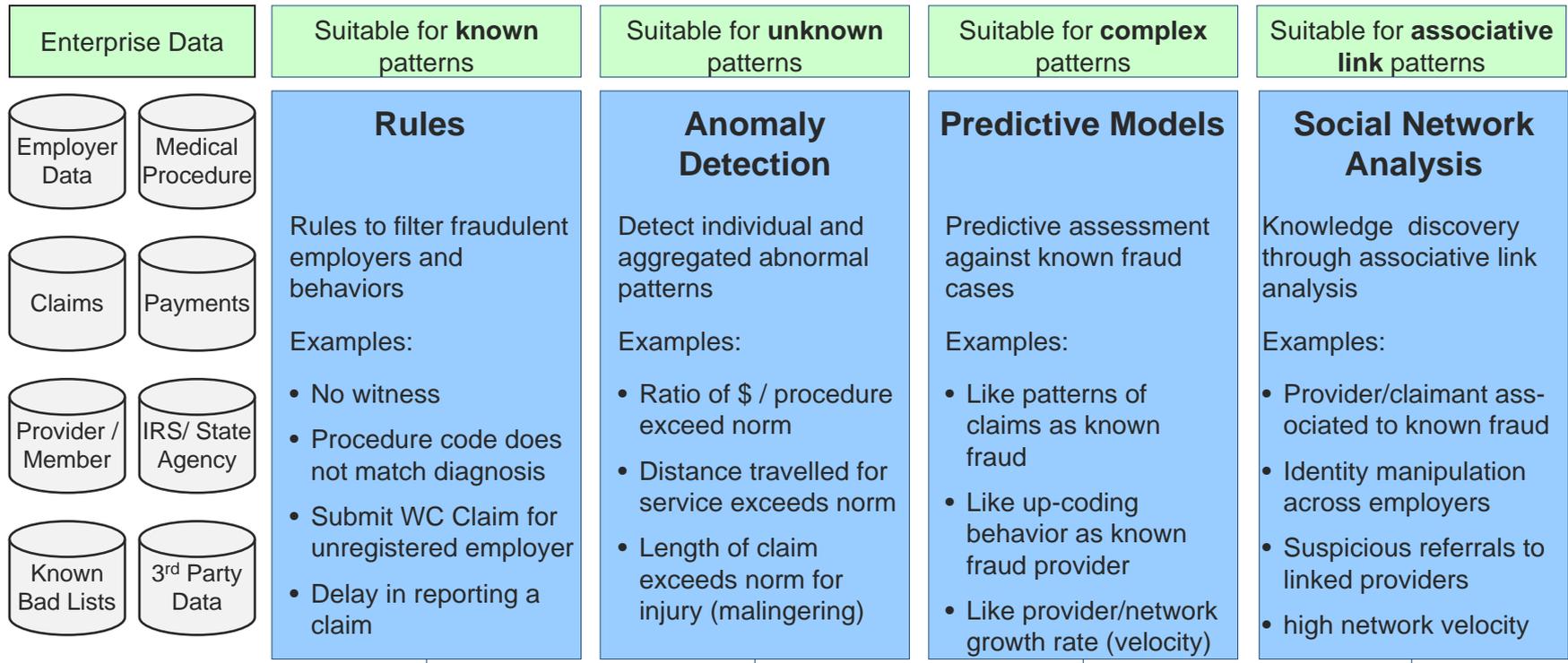
Industry Best Practice – End-to-end Process

Process Flow



Industry Best Practice – Hybrid Analytics

Using a Hybrid Approach for Fraud Detection



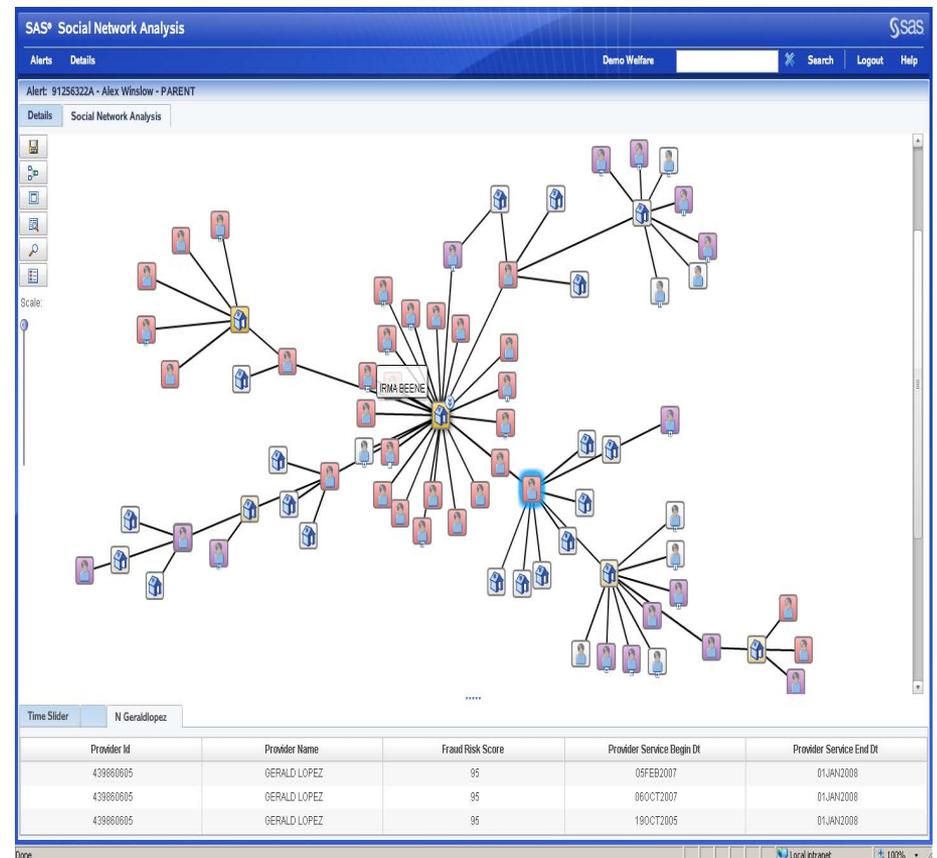
Hybrid Approach

Proactively applies combination of all 4 approaches at entity and network levels

Social Network Analysis – The New Frontier

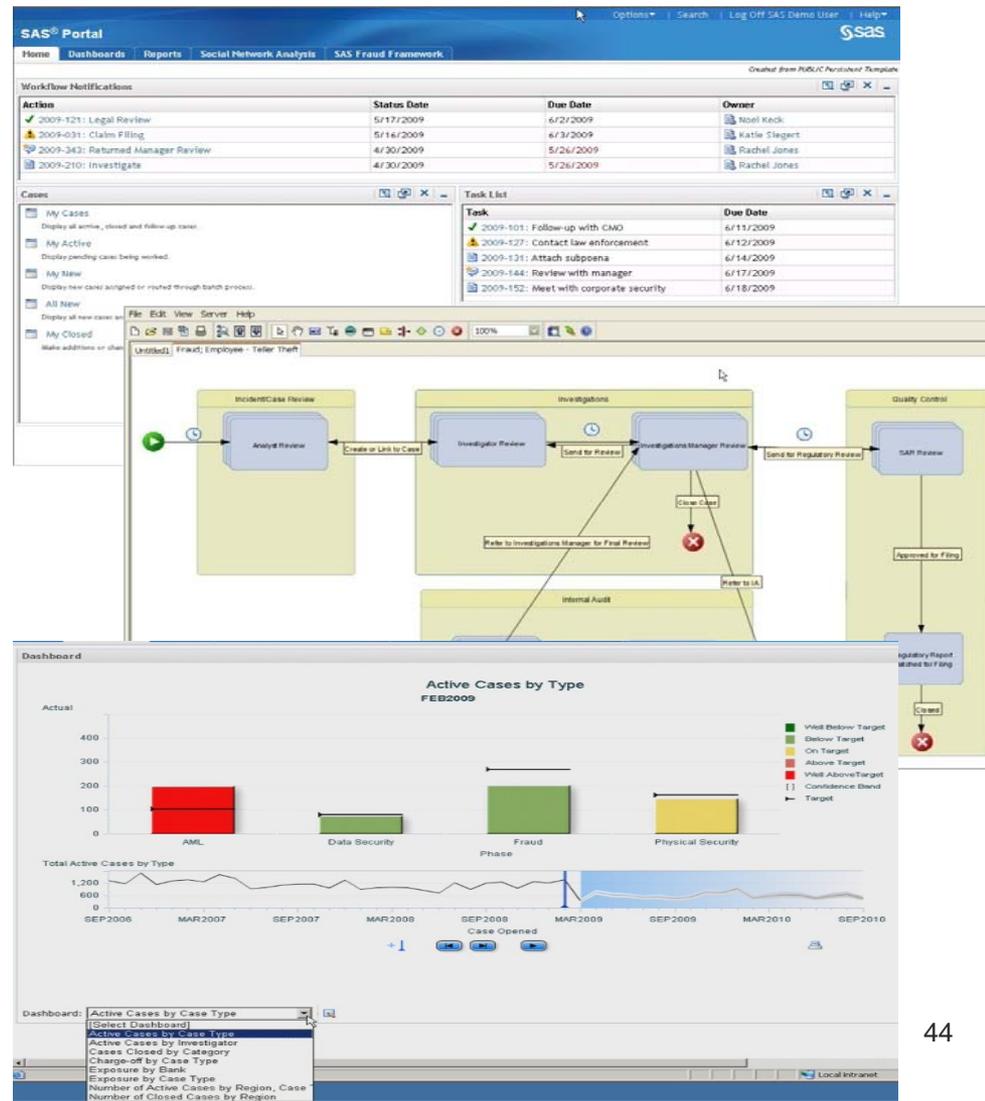
Automatic linking, scoring, and visualization

- Entity Resolution
 - Collapse nominals
 - Single view of entities
- Iterative network build and refinement
 - Statistical binding of entities
 - Soft / behavioral links
- Network scoring & evaluation
 - Rule and analytic-based scoring
 - Configurable prioritization
 - Network visualization



Enterprise Case Management

- Single portal for holistic view of fraud (current & historical cases)
- Permission based access defines user capabilities
- Automated method to define and design fraud processes
- Multiple, customized workflows for various case types & processes
- Critical information in readily consumable format via visual interface
- Customized reports and inter-active dashboard access on- demand

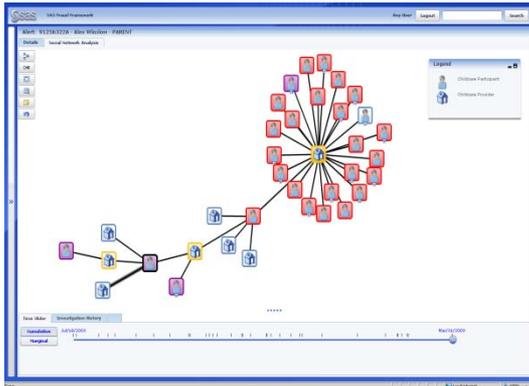


Why an end-to-end Approach with Hybrid Analytics?

Provides the ability to apply Rules, Predictive Models, and Anomaly Detection on linked data

- More fraud/actionable cases identified
 - Including previously undetected opportunistic and organized fraud and network based extensions to already identified cases
- Reduction in false positive rates
 - Holistic information reduces false positives by up to 10+ times over traditional entity centric approaches
- Improved analyst / investigation efficiency
 - Each referral takes 1/2 – 1/3 the time to investigate using network visualization on aggregated data
- Significant increase in ROI per analyst / investigation

Case Study – County Department of Social Services



Highlights

- 32 times increase in # fraud rings detected annually
- Incremental estimated save of \$31.1M annually
- 83% correct hit rate on provider fraud
- 40% correct hit rate on participant fraud
- 6 years of historical data from 5 data source systems

Business Problem

The Department of Social Services of a large US County was being hit by fraud, waste, and abuse across their **public assistance programs**. The County engaged SAS to pilot the **SAS Fraud Framework** to determine if the data analytics and visualization solution could assist in **proactively detecting both opportunistic and organized fraud** across providers and participants in the Childcare program.

SAS Approach

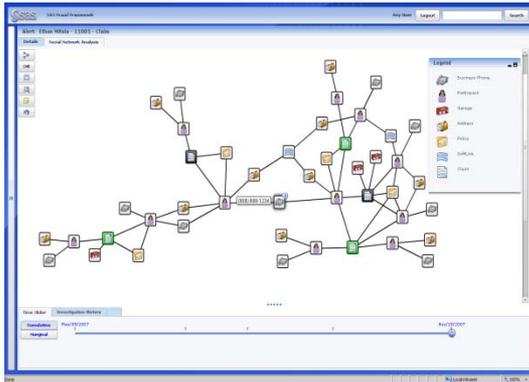
SAS subjected **6 years of historical data** to the predictive capabilities of the SAS Fraud Framework. Client investigators evaluated the solution results during a **3 week validation** period against 4 main categories: **Ease of analyst use, investigative efficiency, earlier fraud detection, and incremental fraud detection.**

Results

The pilot resulted in a business case and deployment roadmap for full implementation:

- **Investigative Efficiency: \$3.0M** (saved across 40 investigators)
 - **Earlier Detection: \$1.6M** annually
 - **Incremental Detection: \$26.5M** annually

Case Study – Workers Compensation Insurer



Highlights

- Advanced analytics drove 35% better results than competition
 - 36% lift on claim referrals
 - 25% lift on network referrals
- Incremental estimated save of \$10.3M annually (for same # of annual investigations)
- 57% lift over current process
- 45% correct hit rate on claims
- 67% correct hit rate on networks
- 100% of WC and GL claims processed (~\$16B claims)

Business Problem

A large US commercial insurer was incurring significant fraud losses across their lines of business. The insurer **engaged 3 vendors in a competitive pilot** to determine the solution that would provide the most lift over their current rules and models and enhance effectiveness of the triage and fraud investigation teams.

SAS Approach

SAS subjected **4 years of historical data** to the predictive capabilities of the SAS Fraud Framework. Client investigators evaluated the solution results during a **3 week validation** period to identify incremental fraud detection at the claim and network levels, reduction in false positives, and enhancements to investigative efficiency.

Results

The key client decisioning factors for vendor selection include:

- **Incremental Detection: \$10.3M annually** (for same number of investigations)
 - **ADVANCED ANALYTICS**, allowing the appropriate **prioritization of investigator time** and **extraction of maximum value**. Using SAS advanced analytics, SAS performed **35% better** than all other vendors.
- **OPEN ARCHITECTURE**, allowing client to become self sufficient vs. other black box + services based approaches (self sufficiency can **result in significant annual savings on services costs.**)



**THE
POWER
TO KNOW®**



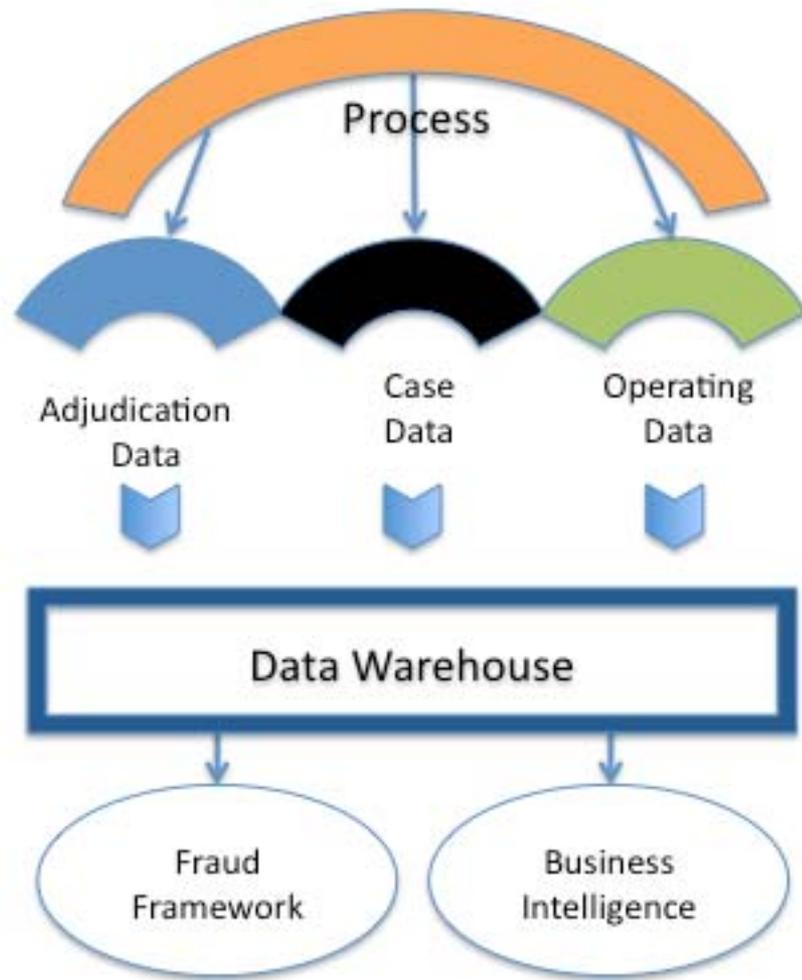
How To Take A Tool and Make It A Solution

Your system's integrity, backed by ours.

M Corp

Create Coherence

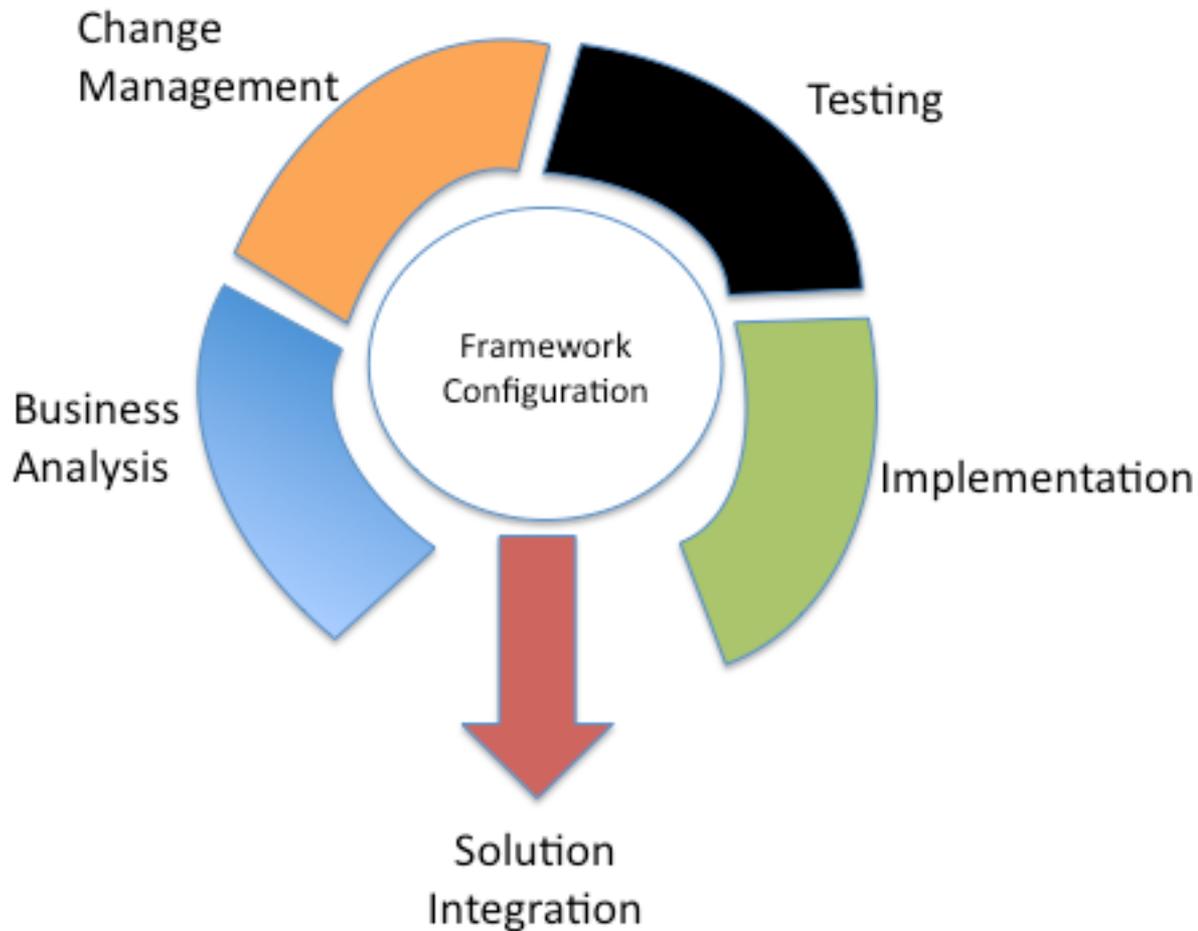
- Processes
- People
- Knowledge
- IT
- Tools



Your system's integrity, backed by ours.

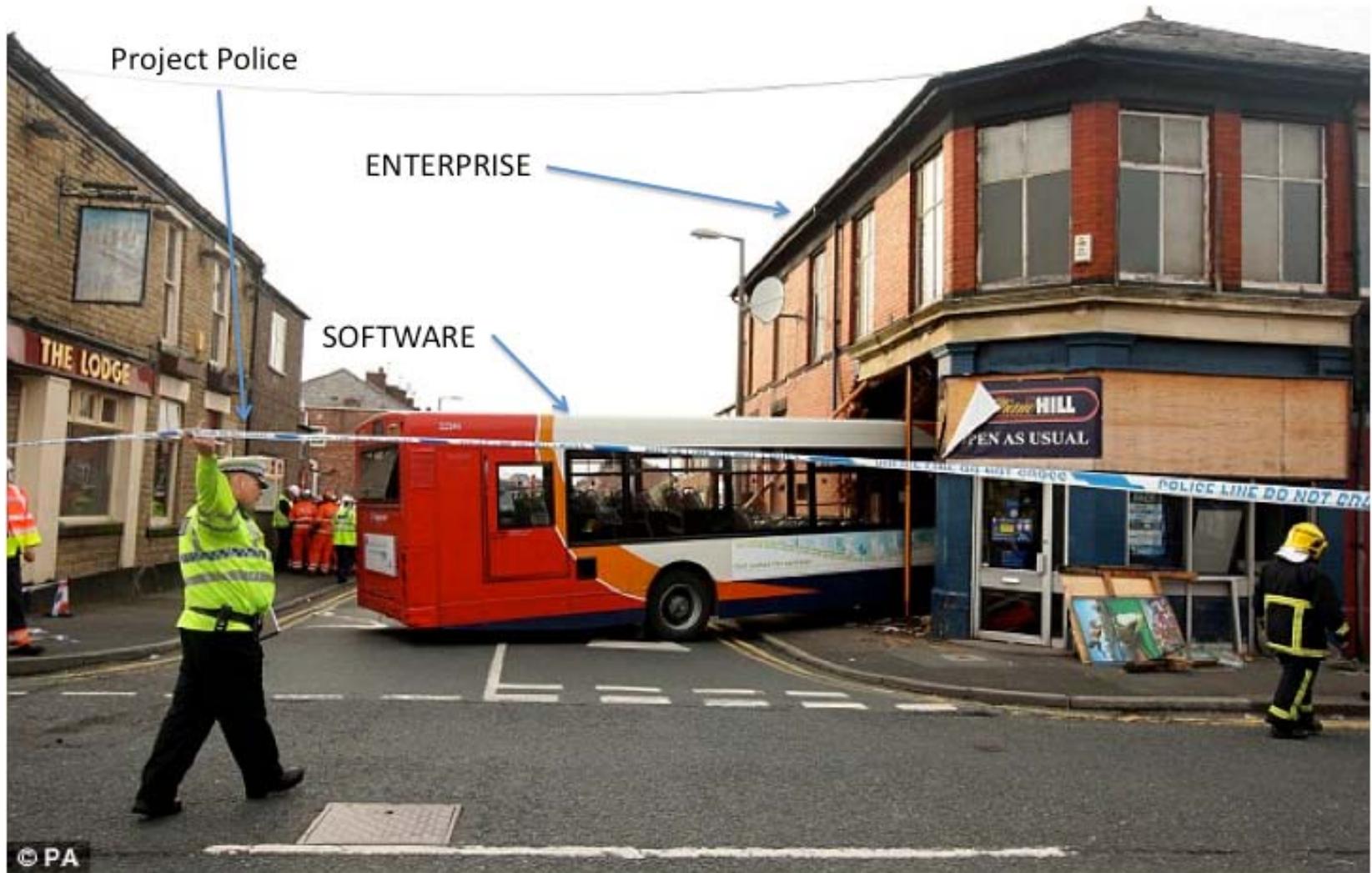
M Corp

Composition of Implementation



Your system's integrity, backed by ours.

M Corp



Your system's integrity, backed by ours.

M Corp



Thank You

Your system's integrity, backed by ours.

M Corp