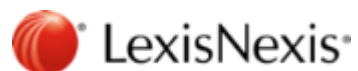




Using Identity Management and Predictive Analytics to Prevent Fraud and Improve Provider and Member Management?

Kathy Mosbaugh, Director, Health Care
February 6, 2013

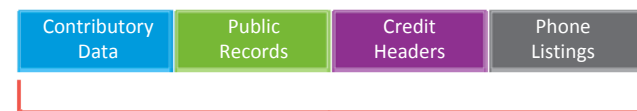


Risk Solutions

© LexisNexis Risk Solutions. All Rights reserved.

LexisNexis leverages data about people, businesses, and assets to assess risk and opportunity associated with industry-specific problems

Identity Authentication and Risk Assessment



Who are you?



Where are you?

How much risk is associated with you?

Insurance	Assess underwriting risk and verify applicant data; prevent/investigate fraudulent claims; optimize policy administration
Financial Services	Prevent/investigate money laundering and comply with laws Prevent/investigate identity fraud
Background Screening	Verify applicant identity and credentials Avoid legal exposure by identifying criminal records and drug use
Receivables Management	Assist collections by locating delinquent debtors Assess collectability of debts and prioritize collection efforts
Legal	Locate/vet witnesses, assess assets/associations of parties in legal actions; Perform diligence on prospective clients (KYC)
Government	Locate missing children/suspects; research/document cases; reduce entitlement fraud; accelerate revenue collection
Health Care	Verify patient identity, eligibility, and ability to pay Validate provider credentials; prevent/investigate fraud

LexisNexis Risk Solutions works with clients across all industries and both federal and state governments



Our Customers

- **100%** of U.S. P&C insurance carriers
- **100%** of the top 50 U.S. banks
- **90%** of the Fortune 500 companies
- **All 50** U.S. states
- **70%** of local governments
- **80%** of U.S. Federal agencies

Health Care Challenges & Trends

Unprecedented risks with EMR adoption, HIEs, ACOs and patient centered medical homes

Sharing of Medical Information Electronically

HIPAA 5010, ICD-10

Administrative burdens

Tougher Rules (CMS 6028-FC) on new provider enrollment and screening standards

Budgetary pressures

PPACA-mandated exchanges

IRS and Patient Protection and Affordable Care Act (ACA) requirements

HIPAA Privacy, Security, Enforcement, and Breach Notification Rules

Interest in Big Data & Analytics

Increasing Government Regulations

Medicaid Expansion

\$2.6 trillion in health care costs

Questionable claims

Stricter Medical Loss Ratio (MLR) requirements

Health Care Fraud Statute (18 U.S.C. §1347)

Improper payments

1.5 million medical identity theft victims

Limited manpower for investigations

of Consumers Entering Health Care System

Labor-intensive costly recovery

Higher insurance premiums

Pursuit to reduce costs

Outdated data and incorrect information

Data security and breaches

HIPAA Privacy, Security, Enforcement, and Breach Notification Rules

“Paying for Care to Dead People”

“Four alleged schemes to defraud MassHealth of \$10 million*found agencies billing taxpayers for care to dead people, widespread kickbacks, or exaggerated claims, prosecutors said.*”

-Boston Herald



“ATC [and others] were charged with various *health care fraud, kickback, money laundering and other offenses*.. so that ATC [and others] could bill Medicare more than \$200 million in medically unnecessary services. “

-FBI News Release

“Real Patients, Real Doctors, Fake Everything Else”

“By inventing 118 bogus health clinics in 25 states, prosecutors said, a band of Armenian-American gangsters billed Medicare for more than \$100 million, and managed to collect \$35 million over at least four years. Charges included *racketeering, health care fraud, identity theft, money laundering and bank fraud.*”

At its heart, the gang, based largely in Los Angeles, *resembled a giant identity-theft ring that stole doctors’ dates of birth and Social Security and medical license numbers and paired them up with legitimate Medicare recipients, whose names and information were also stolen.*

About 3,000 of those patients’ names came from the Orange Regional Medical Center in Middletown, N.Y.”

- NY Times



Past and Current Medicaid Anti-Fraud and Abuse Practices

Pew Center on the States | Pew Charitable Trusts

Database that compiles and categorizes promising practices states employ to combat Medicaid fraud and abuse.

1. Screening them before and after they are accepted into the program;
2. Reviewing claims before they are paid; and
3. Reviewing claims after they are paid and recovering those deemed improper—known as “pay and chase.”

State

All States

Alabama

Alaska

Arizona

Arkansas

California

Colorado

Connecticut

Delaware

District of Columbia

Florida

Georgia

Hawaii

Idaho

Practice Type

Provider Regulation	Prepayment Review	Post Payment Recovery	Cross-Cutting
☒ Provider Accountability	☒ Service Verification	☒ Data Mining	☒ Stakeholder Coordination
☒ Excluding Problem Providers	☒ Prior Authorization and Claims Review	☒ Detection and Investigation	☒ Provider Outreach and Education
	☒ Recipient Lock-In	☒ Penalties and Recovery	☒ Managed Care Oversight
		☒ Medicaid Fraud Control Unit Coordination	☒ Targeting High-Risk Providers

☐ CMS Noteworthy Picks Only

Reset Selections

Search

Source: <http://www.pewstates.org/research/reports/combating-medicaid-fraud-and-abuse-85899445796?p=1>

How Well Do You Know Your Participants....

- For managed care organizations, Medicaid re-enrollment can drop as much as 30% due to incorrect member contact information.
- 5-10% of individual contact information provided by commercial carriers is incorrect.
- 15-20% of individual contact information provided by employers is incorrect.
- 25-30% of individual contact information provided by Medicare is incorrect.
- 40-50% of contact information provided by Medicaid is incorrect.

Deliver Results Across Business Functions



Opportunities

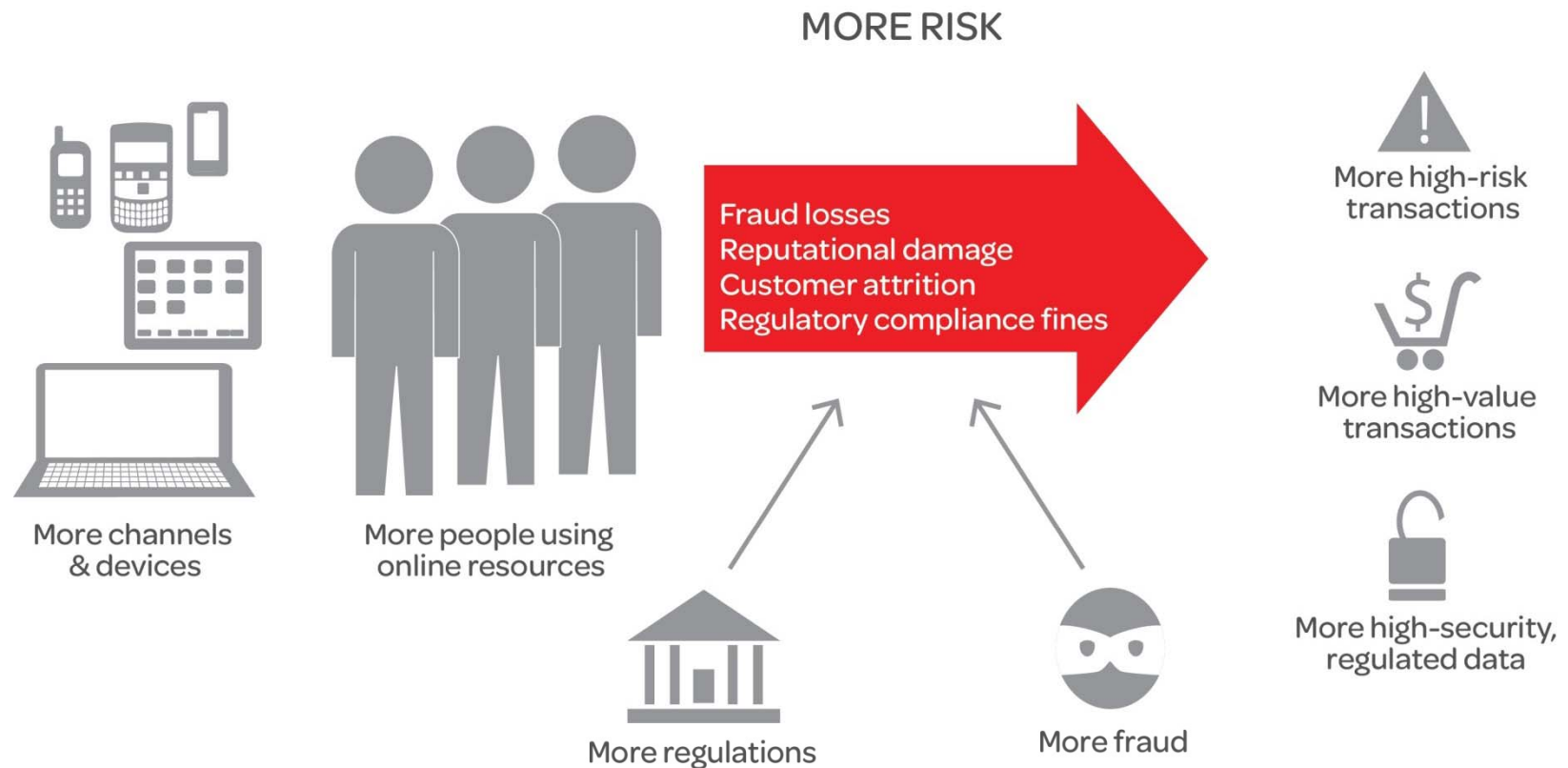
Greater focus on the individuals and entities in the program:

- *Are beneficiaries enrolling who they claim to be?*
- *Have they disclosed all assets, income, correct state of residence, etc?*
- *What are the true backgrounds of the practitioners, officers, agents, etc?*
- *What is the risk profile of a provider based on background, associations, etc.?*
- *What significant events are occurring between enrollment periods?*

Eliminate the “Pay and Chase” status quo by looking to other industries, private sector for successful approaches and technologies like Identity Proofing/Identity Management and Predictive Claims Analytics

The Role of Identity Management

Key Challenge: Commercial, government and non-profit organizations are seeking to provide controlled, secure access to their products, services and information



Comprehensive Identity Management

ENROLLMENT



ASSESSMENT



DISCOVER	Discover the identity Undertake data capture, identity resolution and identity enrichment. <i>"Tell us who you are."</i>
VERIFY	Verify the identity Establish that the identity exists. <i>"Does Bob Jones exist?"</i>
AUTHENTICATE	Authenticate the identity Determine whether an individual or business owns the identity. <i>"Are you Bob Jones?"</i>
EVALUATE	Evaluate the identity Assess against legislation, regulations and rules to determine if an individual or business is eligible. <i>"Is Bob Jones eligible?"</i>
ALERT	Alert to identity changes Receive notification when an individual or business is exhibiting high-risk behavior (continuous evaluation). <i>"Is Bob Jones still eligible?"</i>

Success in the Government segment with Identity Management

Example #1

- Stopped over \$20M in Refund Fraud related to Identity
- Individuals requested refunds for stolen, fabricated or modified identities

Example #2

- Submitted 74,915 debts
- Retuned 61,660 debts with updated information
- Resulted in collections of over \$4 Million

Example #3

- Regularly scrubs addresses for Returned Mail
- Equates to about \$1 Million in additional collections because letters are reaching the intended recipients

Identity Management for Beneficiaries

Reduces beneficiary fraud and ensures accuracy of identity information for program efficiency and risk mitigation

Test Criteria	Fraud Risk
Deceased	High
Incarcerated	High
Identity Fraud Risk	High
Occupancy Outside State	High
Real Property Value and Ownership	Medium
Motor Vehicle Age and Ownership	Medium
High Risk Address	Medium

In a recent analysis of a Medicaid beneficiary file:

- over 2% of beneficiaries had a primary address in another state
- 0.59% were deceased
- 2% of adults presented with severe identity fraud risk

Identity Management for Providers

Maintains visibility into provider risk

Test Criteria	Fraud Risk
Deceased	High
Medicare Exclusion List (LEIE)	High
GSA Exclusion List (EPLS)	High
Felony conviction	High
State of Licensure, status	Medium
Known Associates Excluded	Medium

In a recent analysis of a Medicaid provider file:

- Over 1% were deceased
- 1.7% of providers were sanctioned
- Incarcerated individuals were active providers
- **Undisclosed associations to excluded providers were identified**

An Approach to Comprehensive Provider Management

Program Integrity begins with **knowing** your providers

Screen all enrolled fee-for-service providers



Implement robust provider validation and evaluation upon enrollment



Assign dynamic risk scores and track provider files between enrollment periods for pertinent activity; alerts generated for changes



Extend enrollment and screening standards to include managed care organizations

Deliver Results Across Payer Functions



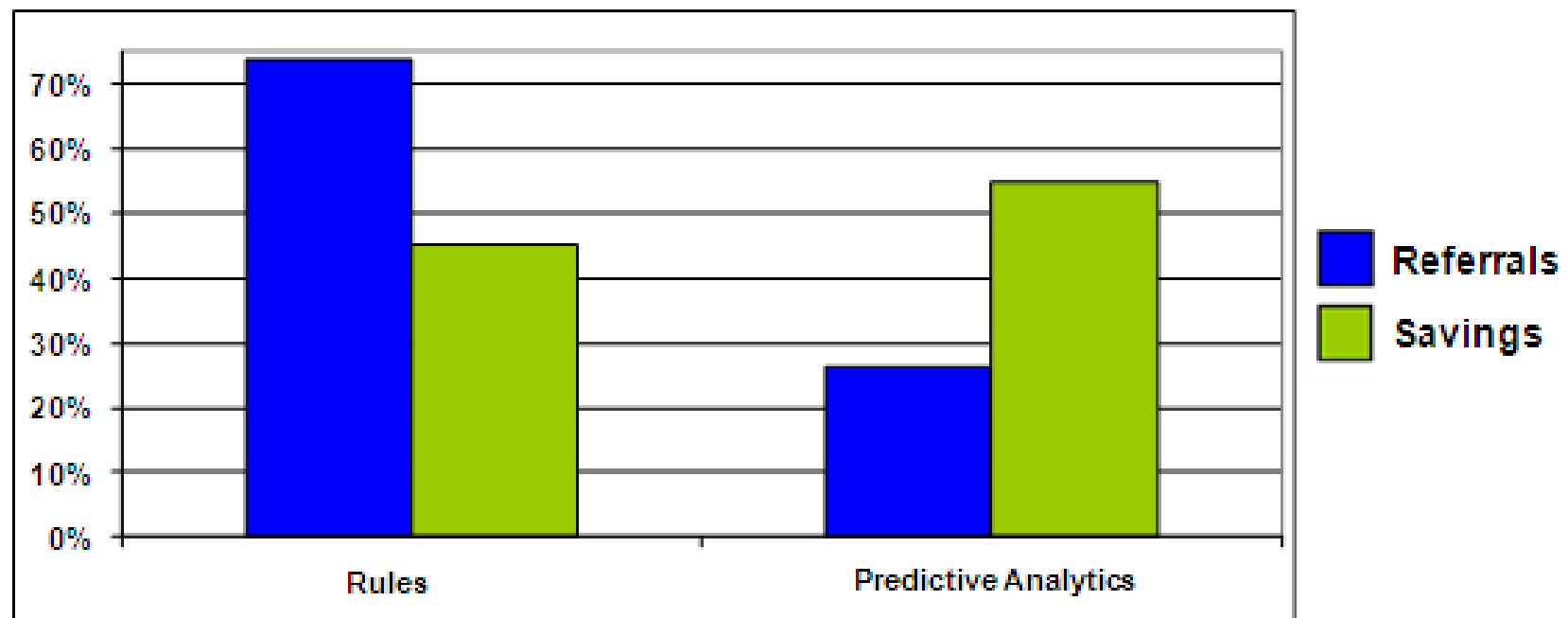
The National Health Care Anti-Fraud Association (NHCAA) conservatively estimates that about 3 percent of U.S. healthcare spending is lost to fraud or payment and billing errors.

NHCAA also estimates that about 70 percent of payers use some form of anti-fraud system, with many still using the “pay and chase” methodology.

Source: <http://www.healthcarepayernews.com/content/unitedhealth-touts-predictive-modeling-solution-healthcare-fraud-and-preventable>

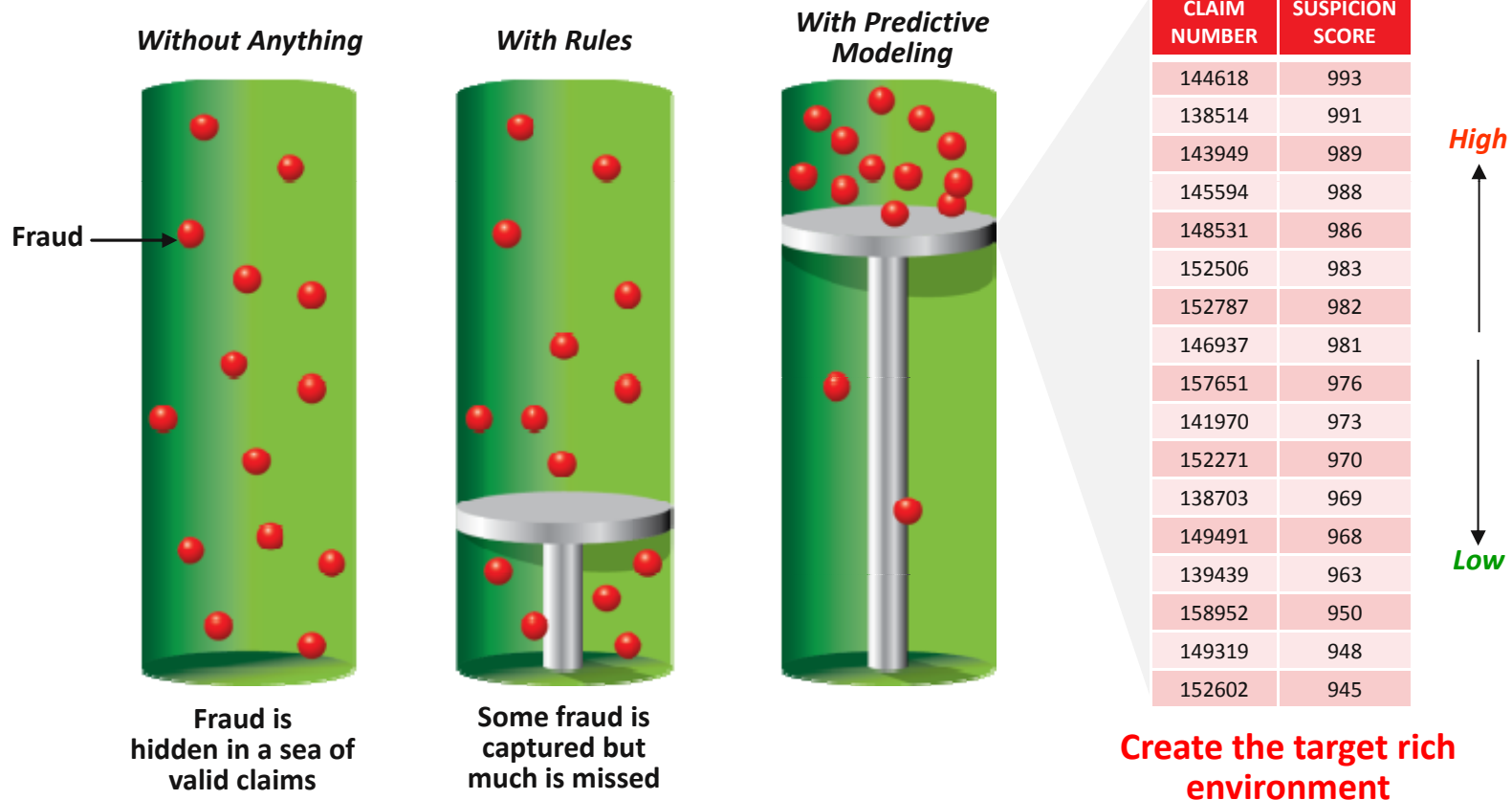
Our Customer's Experience...

- ROI's tend to rise over time; ROIs usually start in the mid-single digits and move up to double digits with experience
- With most of our clients, LexisNexis risk alerts lead to 30-40% of all the referrals accepted into their SIU's and are usually the higher cost referrals



Claim Scoring Using Predictive Models

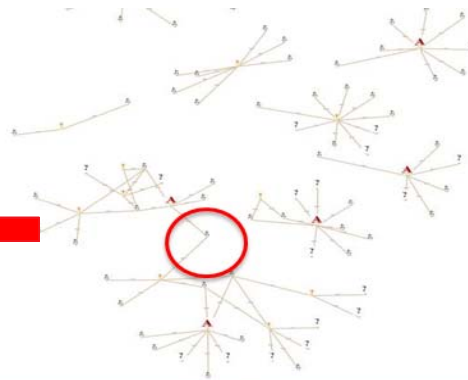
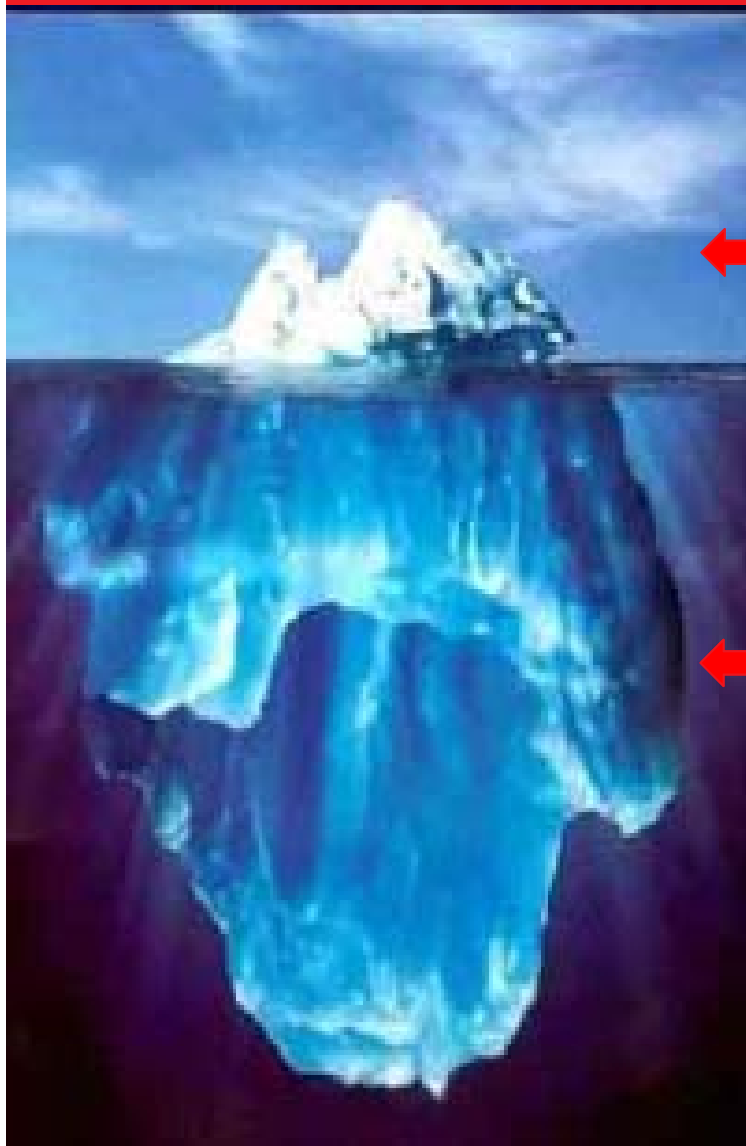
Predictive analytics provides a score for each claim, policy, etc., allowing activity to be concentrated on areas that have the highest probability of financial return.



Social Network Analytics Helps Make Sense of Big Data

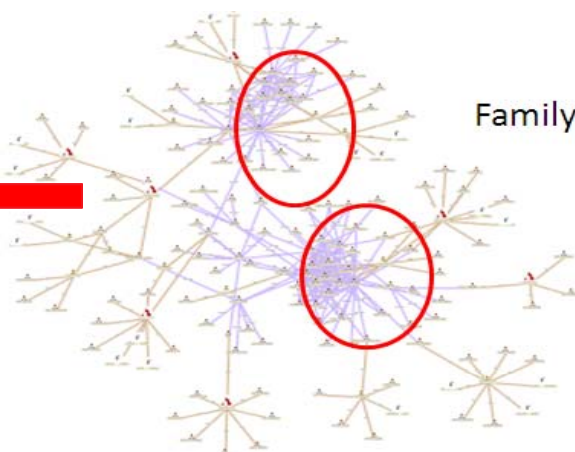
- Social Network Analysis identifies relationship clusters leveraging “big data” and advanced linking to reveal the relationships that criminal networks try so hard to keep hidden, enabling the effective investigation and termination of insidious and costly fraud rings
- Social Network Analytics can reveal
 - Patient relationships with known perpetrators of health care fraud
 - Links between recipients, businesses, and assets, as well as relatives and associates
 - Links between licensed and non-licensed providers
 - Suspect relationships of employees, suppliers, and partners with patients and providers

Social Network Analytics Get Below the Surface



Traditional investigation and relationship analytics tools without linking technology only scratch the surface of fraudulent activities.

7 claims @ an average of \$200,000 each = \$1.4M



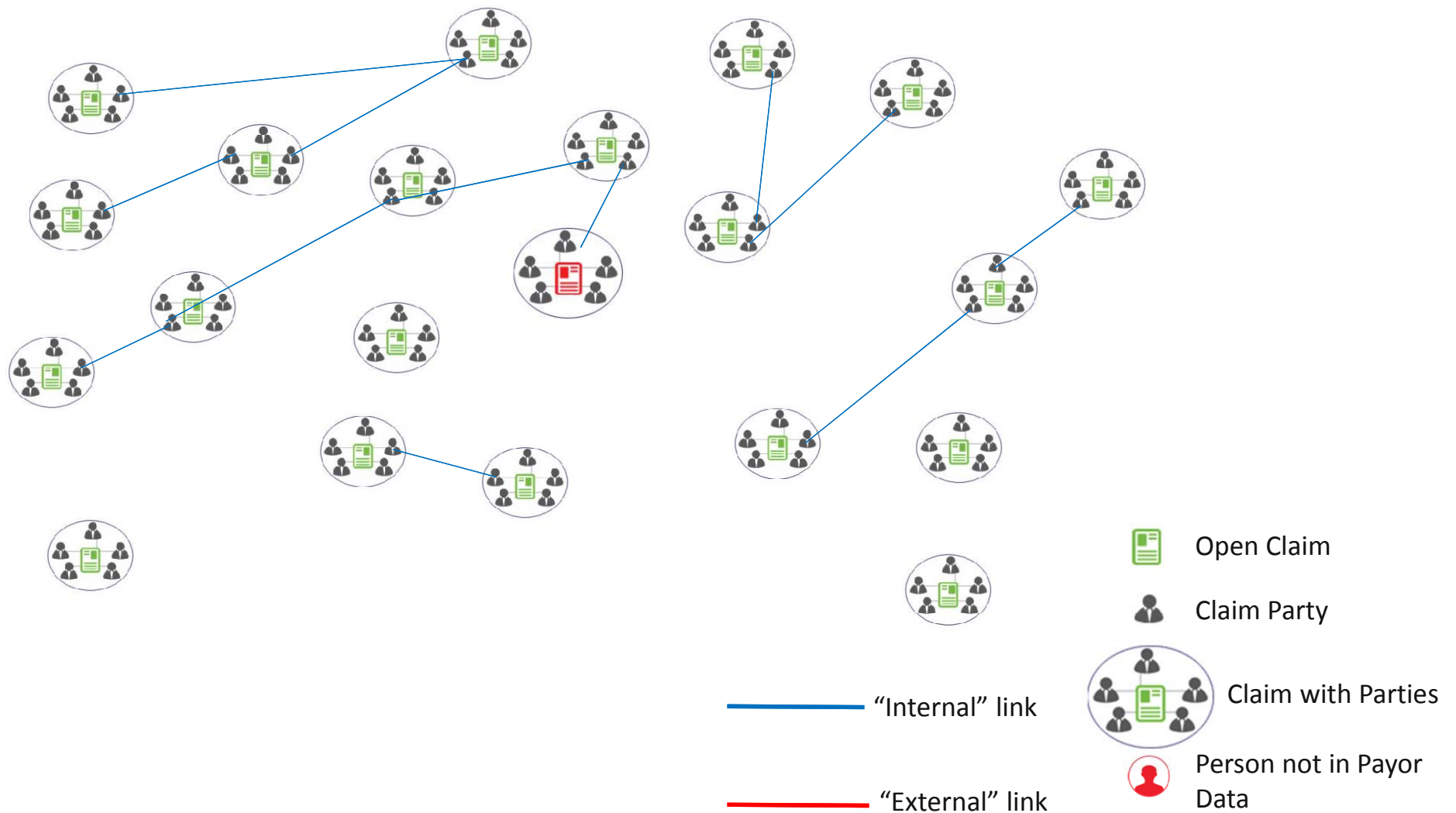
Family 1

Family 2

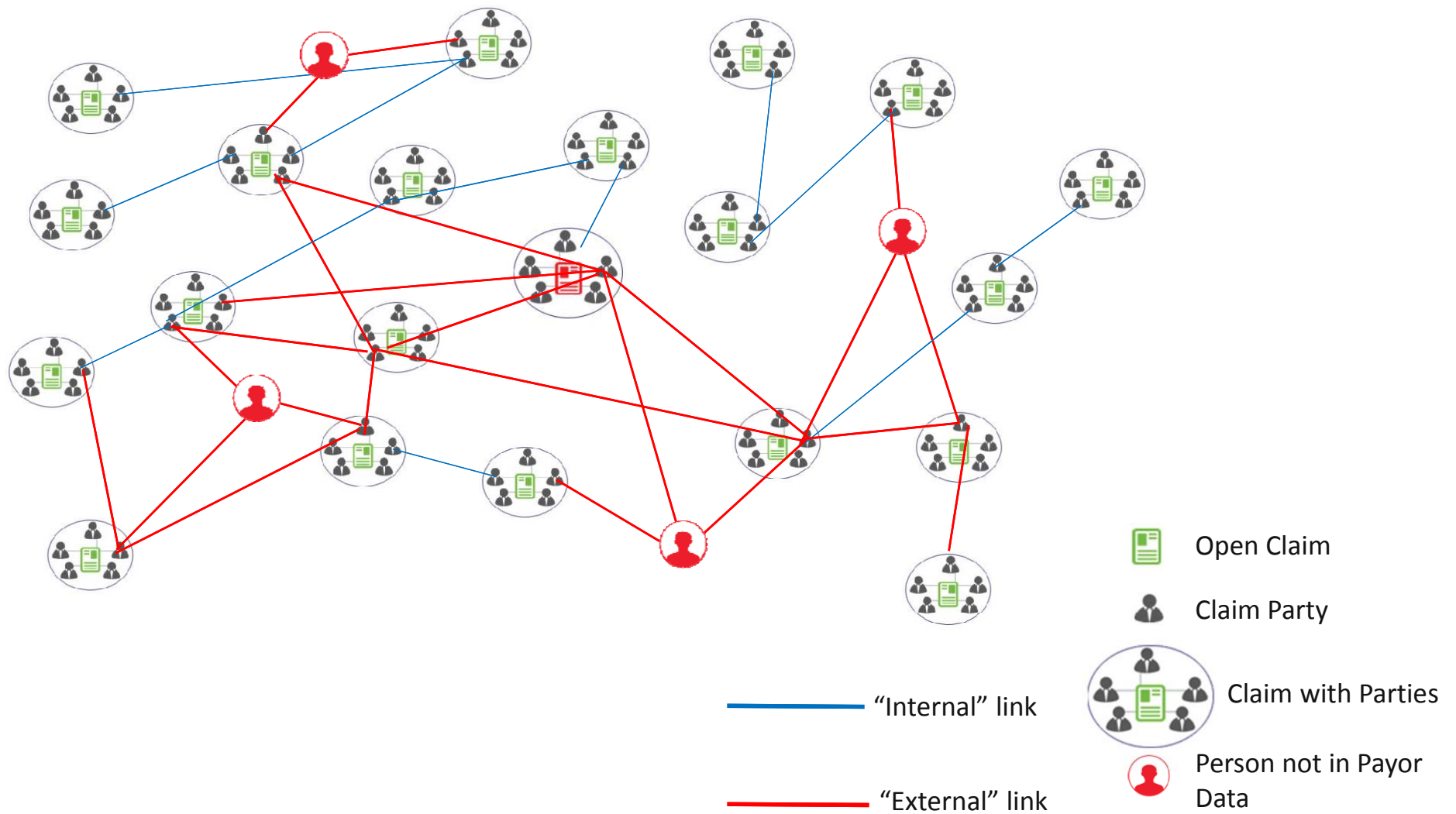
Next generation relationship linking analytics allows you to get below the surface to find collusive behavior not otherwise visible, dramatically increasing potential for savings.

18 claims @ an average of \$200,000 each = \$3.6M

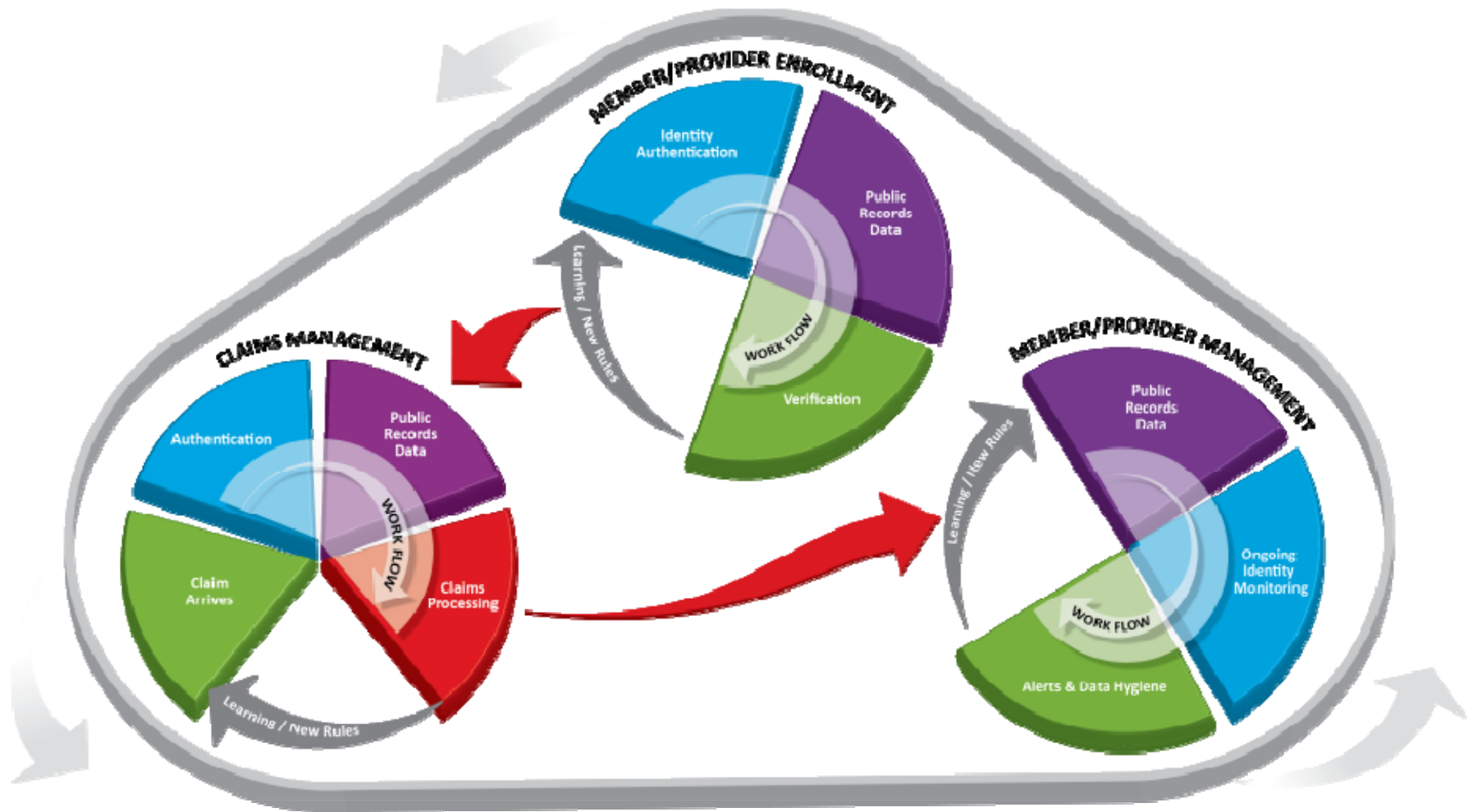
Discovering the Missing Links



Discovering the Missing Links



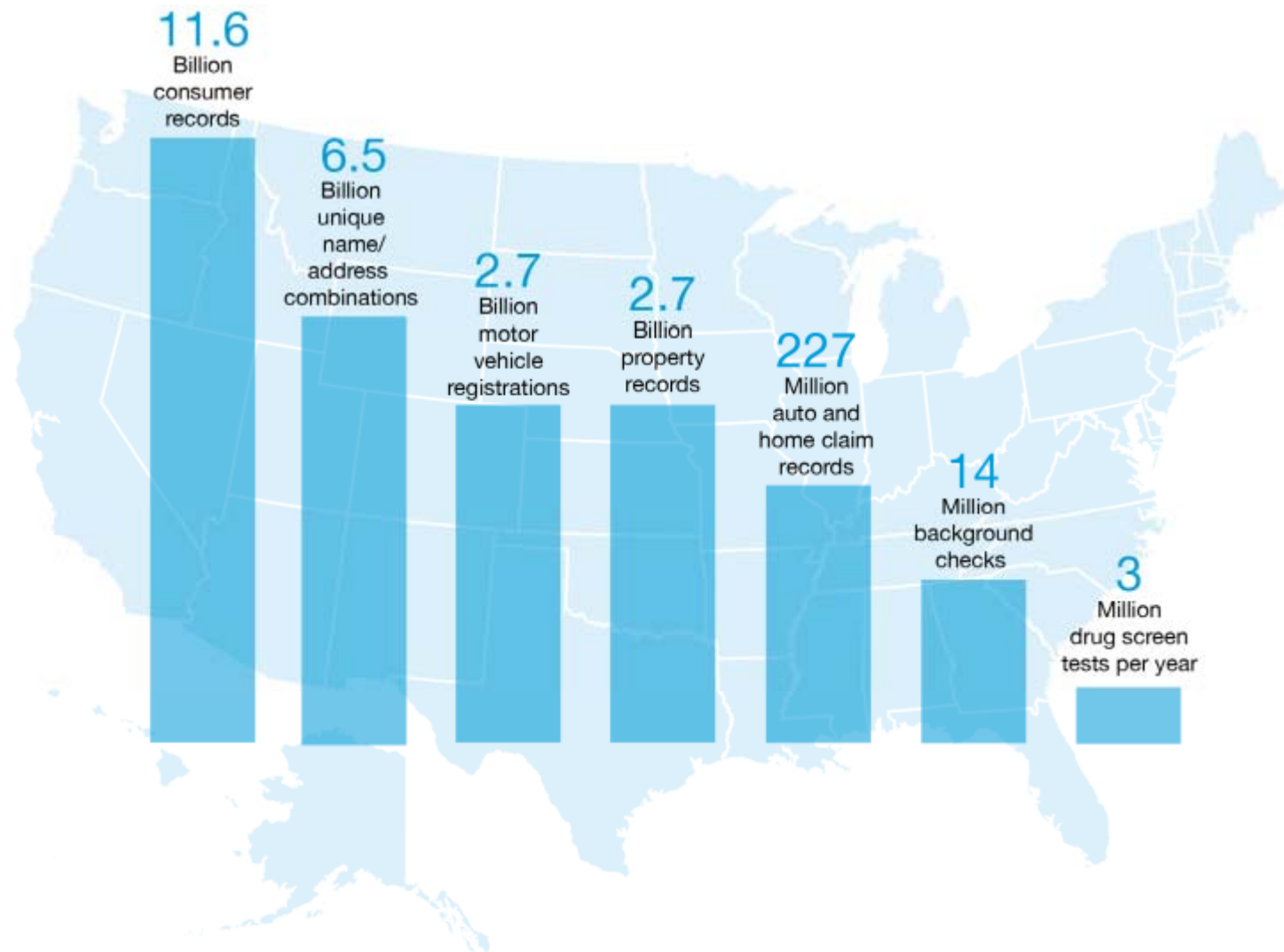
Holistic Approach to Risk Management Across Processes Yields Improved Results



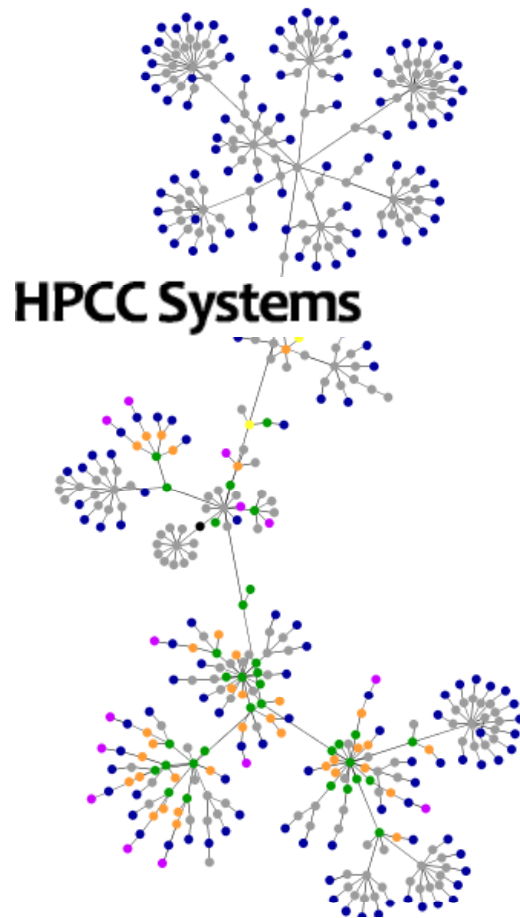
Thank You

Appendix

LexisNexis Risk Solutions has billions of public and proprietary data on hundreds of millions of individuals and businesses



LexisNexis High Performing Computing Clusters (HPCC)



Powered by HPCC Systems™, the LexisNexis massive parallel-processing open-source computing platform.

Graph \ Network 3 Billion derived public data relationships between people merged with risk indicators.

Graph Analytics examine up to 20 billion data points to create variables that allows for predictive analysis incorporating relationship context and associated risk.

Targets fraud across all sectors including Health Care, Financial Services and Government.

Unique Identifier

LexIDSM

The fastest linking technology platform available with results that help you make intelligent information connections.

LexIDSM is the ingredient behind our products that turns disparate information into meaningful insights. This technology enables customers using our products to identify, link and organize information quickly with a high degree of accuracy.



Get a more complete picture

Make intelligent information connections beyond the obvious by drawing insights from both traditional and new sources of data.

Better results, faster

Use the fastest technology for processing large amounts of data to help you solve cases more quickly and confidently.

Protect private information

Keep customer SSNs and FEINs secure and enjoy peace of mind knowing you are taking steps to observe the highest levels of privacy and compliance.