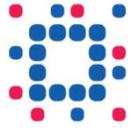




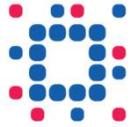
## Experian/SAS Architecture for FCC

June 28, 2012



# Agenda

- Introductions
- Notional Process Flow for Eligibility Determination and Verification of Identity
  - ▶ The Problem
  - ▶ Conceptual Process Flow
- Program Integrity Components
  - ▶ Experian
    - ID Proofing
    - Comprehensive Datasets
  - ▶ SAS
    - SAS Fraud Framework
    - SAS Real-Time Analytics
    - SAS Case Management
- Analytic Detection Engine Examples



## The Problem:

- Currently are three types of calls into IP Relay Service Centers that are ultimately reimbursed by FCC:

Legitimate Enrollees



Tara: The SSA has certified her bilateral hearing capabilities are under 40 decibels and she'd like to order some things from a local store.



Sophisticated Criminals



Taylor: His hearing is just fine, and he's completely hacked Tara's email accounts obtaining ID and financial information and is placing an order for several Dell computers in her name.



Unsophisticated Criminals

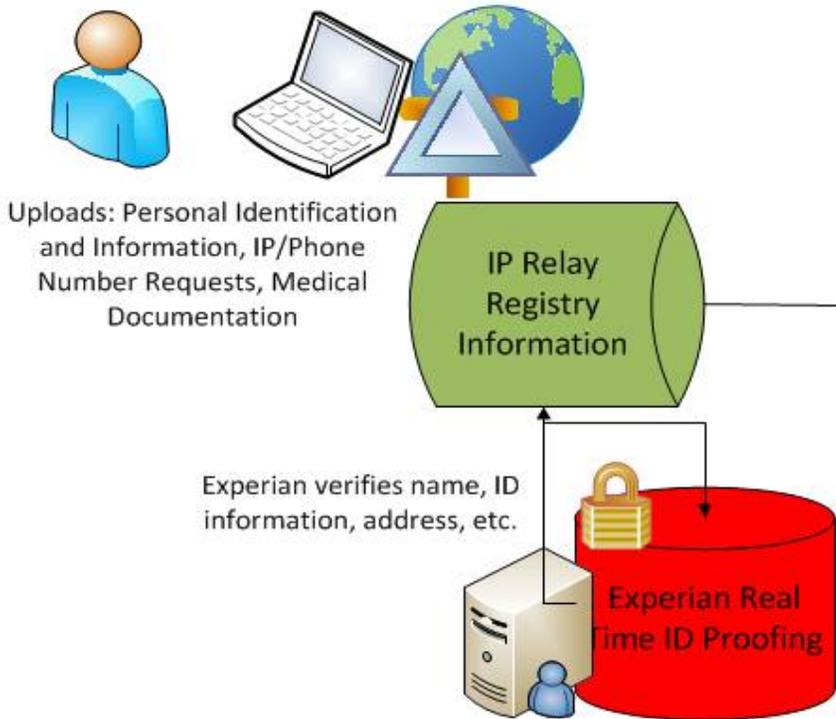


Steven: Like Taylor, his hearing is just fine. Steven, however, doesn't hack the information himself. He simply purchases ID numbers of program enrollees or obtains false documentation that qualifies him for entry into the IP Relay Service program so he can order products with stolen credit cards

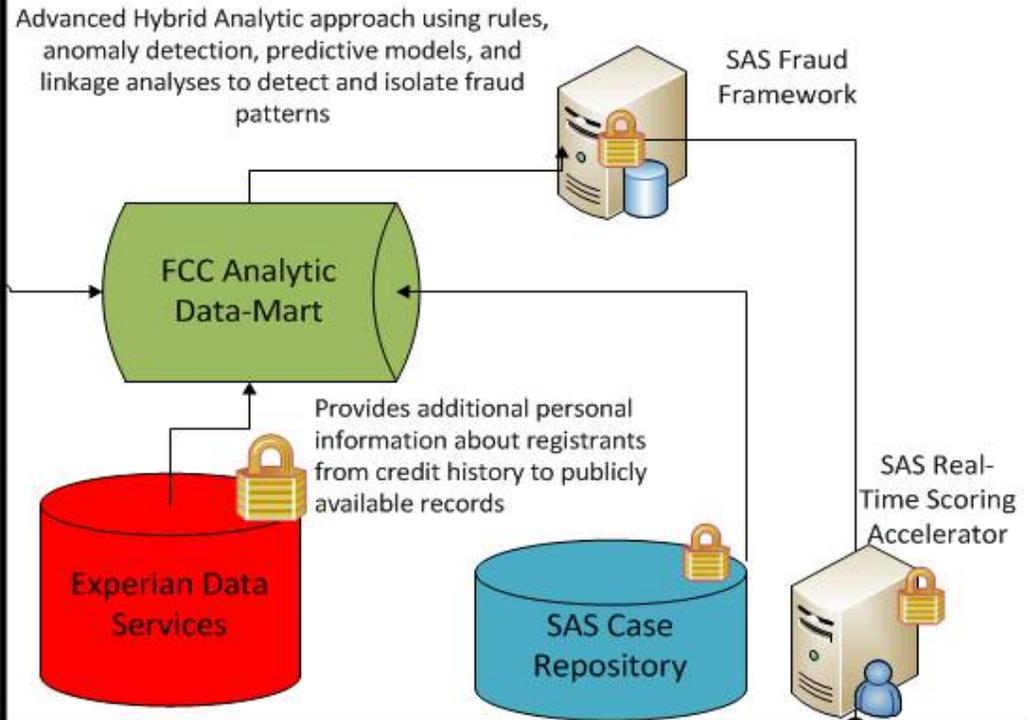


- FCC needs a comprehensive strategy to detect and properly classify every IP Relay call into one of these buckets to ensure that carriers spend their efforts connecting calls of legitimate program enrollees

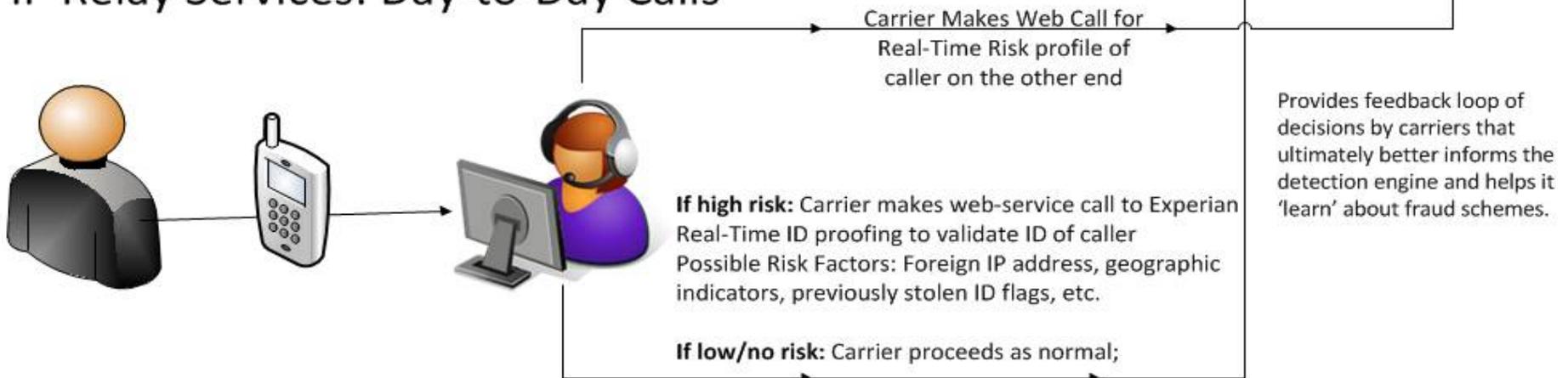
## Registration for IP Relay Services

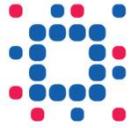


## Real-Time Detection of Criminal Calls



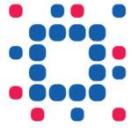
## IP Relay Services: Day-to-Day Calls





## Program Integrity Components:

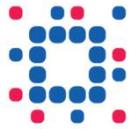
- Program Integrity Components
  - ▶ Experian
    - ID Proofing
    - Comprehensive Datasets
  - ▶ SAS
    - SAS Fraud Framework
    - SAS Real-Time Analytics
    - SAS Case Management
- Analytic Detection Engine Examples



# Experian: Risk-based approach to identity proofing

## Elements and value proposition

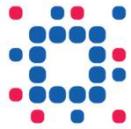
Element	Description	Value
<b>Summary</b> Detailed and summary-level consumer authentication results	Consumer authentication summary and detailed-level outcomes that portray the level of verification achieved across identity elements such as name, address, Social Security number, data of birth and phone	Delivers a breadth of information to allow positive reconciliation of high-risk fraud and/or compliance conditions  Specific results can be used in manual or automated decisioning policies as well as scoring models
<b>Strategy</b> Flexibly-defined decisioning strategies and process	Data and operationally-driven policies, including KBA, that can be applied to the gathering, authentication and level of acceptance or denial of consumer identity information	Employ consistent policies for detecting high-risk conditions, reconciling those conditions that can be, and ultimately determine, the response to authentication results whether it is acceptance or denial of access  Adjust as operational policies warrant



## Experian: Key Precise ID output elements

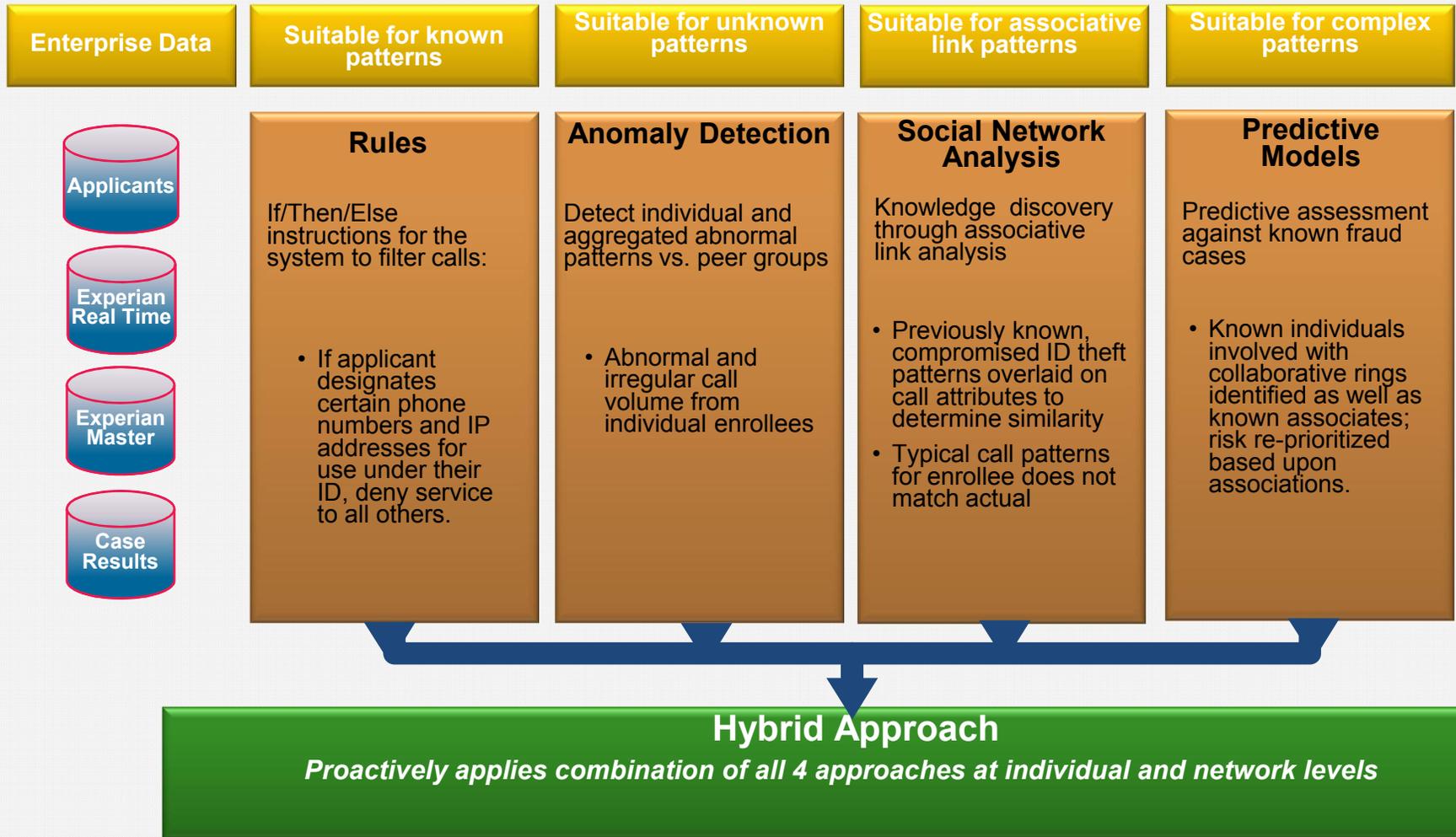
- Checkpoint results – consumer demographic summary and detail
  - ▶ Match level codes
  - ▶ Additional addresses, consumers, phone, DOB, SSN info
- Fraud Shield indicators
- Shared application conditions
- National Fraud Database
- Fraud classification
- IP address verification and detail
- Credit card verification
- Scores and score factors
- Out of wallet questions
- Decisioning

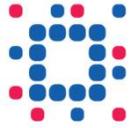




# SAS Fraud Framework for IP Relay Services

## Using a Hybrid Analytic Approach for Filtering IP Relay Phone Calls





**SAS:**

## Analytic Detection Engine Examples:

- Bank of America (BoA):
  - ▶ SAS hosts an environment that performs near-real time scoring on over 8 billion daily BoA credit and debit card transactions.
- Internal Revenue Service (IRS):
  - ▶ SAS is contracted to design and build a near-real time advanced analytic environment for compliance detection across all personal income tax returns.
- Center for Medicare Services (CMS):
  - ▶ SAS was contracted to detect fraudulent claims in the Home Health program. Using 32 previously successful prosecutions, we identified 4 distinct fraud patterns. We then overlaid those patterns on new claims data to provide 54 recommendations for investigation.



# SAS:

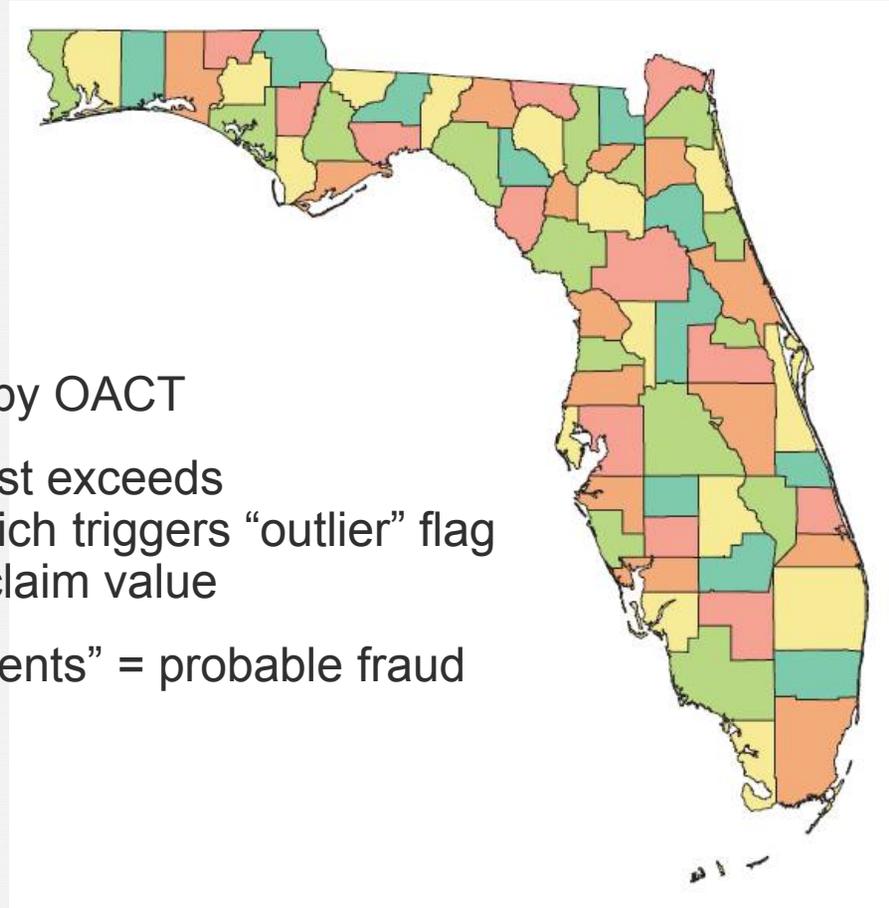
## The Hybrid Approach at IRS

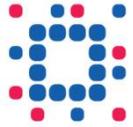
- Enterprise Data Management
  - ▶ Public record datasets – EITCs are flowing out the door because prisoners file taxes from friend/family addresses. SAS will link third party data as part of Enterprise Data strategy
- Rules
  - ▶ Tax laws – Examples abound; if an individual earns over 70k per year, then they are not eligible to deduct student loan interest
- Anomaly Detection
  - ▶ Under-reporting of wages – Comparisons by job category, geographic area, market earnings, etc. allow us to detect outliers in the tax return data
- Predictive Modeling
  - ▶ Known TIN theft schemes overlaid on new tax returns to determine statistical similarity and prevention of identify theft before returns are paid.
- Social Network Analysis
  - ▶ Ghost Return Preparers – The Tax Preparer doing taxes for cash on the side and doesn't sign individual returns with their information. IRS needs to detect when this occurs



## SAS: CMS Project Background - Scope

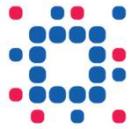
- Fraud project focused on Florida HHA providers
  - ▶ Florida was the only location with a list of known fraudsters (32)
  - ▶ HHA Fraud in Florida is heavily characterized by outlier payments
    - Definition of target provided by OACT
    - “Outlier Payment” = claim cost exceeds predetermined threshold, which triggers “outlier” flag & government pays 80% of claim value
    - 40% or greater “outlier payments” = probable fraud





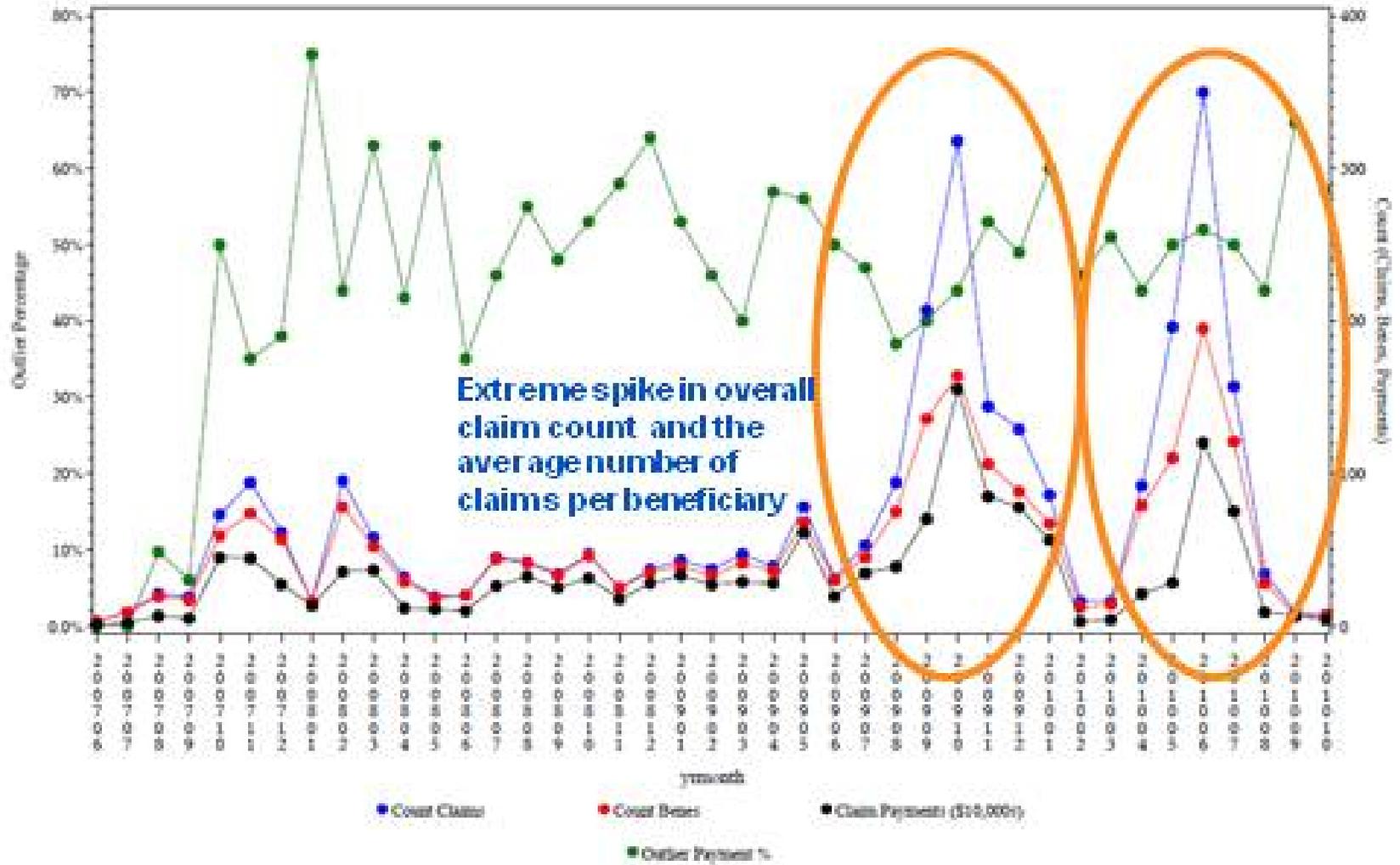
## SAS: CMS Project Highlights - Results

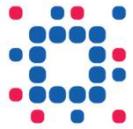
- 18 competing models were created
  - ▶ More than 40 variables included as model inputs
  - ▶ 3 target definitions (2 addressed in this presentation)
- 4 patterns of questionable or suspicious provider behavior were identified using historical claims data
- Top 5% of scored providers captured:
  - ▶ Additional \$800M potentially at risk
  - ▶ 54 additional potential fraudulent providers



# Sophisticated Criminal – Mr. Calculating

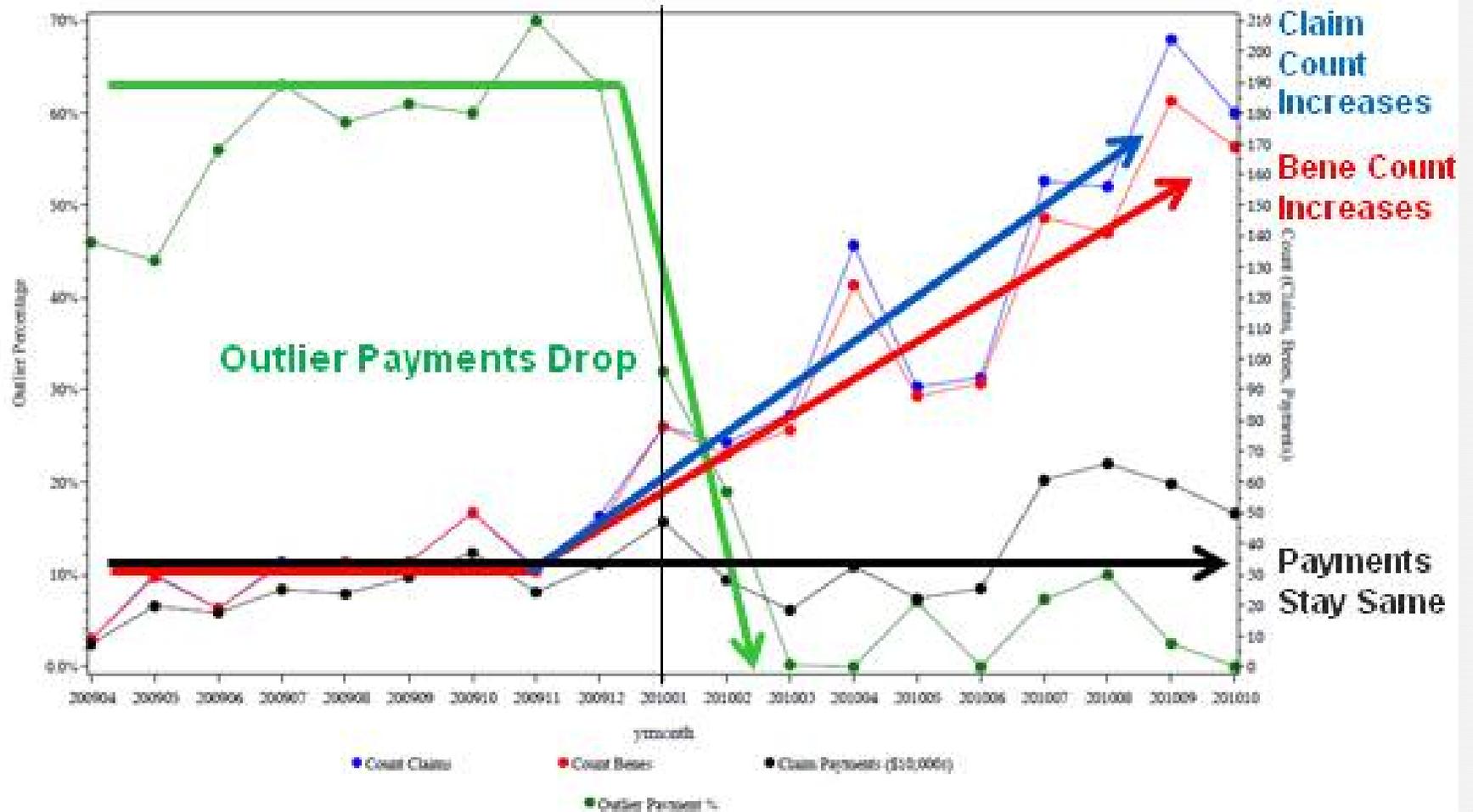
HHA Provider: Claims, Beneficiaries, Payments, and Outlier %

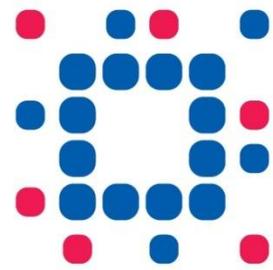
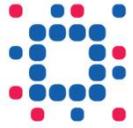




# Unsophisticated Criminal: Mr. Obvious

HHA Provider: Claims, Beneficiaries, Payments, and Outlier %





# Experian

A world of insight