Today’s presenters

Jill Reyes
Director, Risk Advisory Services
RSM US LLP
Melbourne, Florida
jill.reyes@rsmus.com
+1 321 751 6228

Laura Manlove
Manager, Risk Advisory Services
RSM US LLP
Melbourne, Florida
laura.manlove@rsmus.com
+1 321 751 6254
Agenda

• Fraud Refresher
• Overview of data analytics in the anti-fraud and fraud investigation context
• Capability limitations of traditional data analytics methods and how to overcome
• The power of combining publicly available information and data visualization technology
• Real world examples of indications of fraud identified using advanced data analytics, public information and visualization technology
Fraud Refresher – Why are we here?
The term *fraud* is defined in *Black's Law Dictionary* (Eighth Edition, 2004) as:

A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment.
No free lunch...

• In terms of number of reported cases in an industry, governments are the second most frequent, topped only by the banking industry.

• Business fraud and abuse in the U.S. cost about $900 billion a year
  – Educational organizations lose an average of $58,000 per fraud scheme
  – Average organization loses 5% of revenue
  – 58% recover nothing after fraud is discovered

• Street crime only costs the U.S. $4 billion annually

Source: Association of Certified Fraud Examiners, Report to the Nations on Occupational Fraud & Abuse 2014
Just the Facts...

- Fraud schemes frequently continue for years before they are detected, with an average time of 18 months.
- Frauds are much more likely to be detected by a tip than by audits, controls or any other means.
- The most prominent organizational weakness that contributed to the frauds in our study was a lack of internal controls, which was cited in 29.3% of cases, followed by an override of existing internal controls (more than 20% of cases).
- Occupational fraudsters are generally first-time offenders.
- Average losses in the US have increased 20% in 2 years – from $100K in 2014 to $120K in 2016.
- In the Government cases reported in 2016, 38.4% of cases were for Corruption, 25.3% were billing schemes, followed by Expense Reimbursement (15.7%).

Source: Association of Certified Fraud Examiners, Report to the Nations on Occupational Fraud & Abuse 2014
The Fraud Triangle

- Unrealistic deadlines
- Unrealistic performance goals
- Personal vices

Inadequate or no:
- Supervision & review
- Segregation of duties
- Management approval
- System controls

a.k.a. Rationalization – reconciling behavior with commonly accepted notions of decency & trust.
The Fraud Diamond

**Inadequate or no:**
- Supervision & review
- Segregation of duties
- Management approval
- System controls

**Pressure**
- Unrealistic deadlines
- Unrealistic performance goals
- Personal vices

**Convinced self that fraudulent behavior is worth the risk.**

**Necessary traits and ABILITIES to be right person to pull it off**
- Recognized this particular fraud opportunity and can turn it into reality.
The Nature of the Industry...

- Fraud can be explained by three factors:
  - A supply of motivated offenders
  - The availability of suitable targets
  - The absence of capable guardians or a control system to “mind the store”

- The **opportunity** to commit and conceal fraud is the **only** element over which you (management/leadership) have significant control.

- What can we do about it?

Source: “Red Flags for Fraud” by Mark P. Pattison, Deputy Comptroller, State of New York
In 2014, the % of Government cases was 15.1%, with a median loss of $90K. As shown below, those numbers are on the rise.

Source: Association of Certified Fraud Examiners, Report to the Nations on Occupational Fraud & Abuse 2016
While tips are still the highest method of fraud detection, Management Review and Internal Audit procedures represent nearly 30% of detection. This would include performance of data analytics over high risk categories of transactions. The % of cases detected by tips increases to 47% when there is an anonymous hotline.

Source: Association of Certified Fraud Examiners, Report to the Nations on Occupational Fraud & Abuse 2016
Fraud Detection - Government vs All Cases

Detection of Fraud

<table>
<thead>
<tr>
<th>Type of Detection</th>
<th>Government</th>
<th>All Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tip</td>
<td>46%</td>
<td>43%</td>
</tr>
<tr>
<td>Internal Controls</td>
<td>12%</td>
<td>25%</td>
</tr>
<tr>
<td>Internal Audit</td>
<td>15%</td>
<td>14%</td>
</tr>
<tr>
<td>Accident</td>
<td>5%</td>
<td>7%</td>
</tr>
<tr>
<td>External Audit</td>
<td>7%</td>
<td>7%</td>
</tr>
<tr>
<td>Other</td>
<td>15%</td>
<td>6%</td>
</tr>
</tbody>
</table>

Source: Association of Certified Fraud Examiners, Report to the Nation on Occupational Fraud & Abuse 2014
What are the Fraud Schemes?

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corruption</td>
<td>40%</td>
</tr>
<tr>
<td>Non-cash</td>
<td>23%</td>
</tr>
<tr>
<td>Billing</td>
<td>20%</td>
</tr>
<tr>
<td>Expense Reimbursements</td>
<td>13%</td>
</tr>
<tr>
<td>Cash on Hand</td>
<td>13%</td>
</tr>
<tr>
<td>Skimming</td>
<td>10%</td>
</tr>
<tr>
<td>Payroll</td>
<td>8%</td>
</tr>
<tr>
<td>Financial Statement Fraud</td>
<td>8%</td>
</tr>
<tr>
<td>Cash Larceny</td>
<td>7%</td>
</tr>
<tr>
<td>Check Tampering</td>
<td>6%</td>
</tr>
<tr>
<td>Register Disbursements</td>
<td>3%</td>
</tr>
</tbody>
</table>

Source: Association of Certified Fraud Examiners, Report to the Nation on Occupational Fraud & Abuse 2014
What’s the cost?...

• Economic costs:
  – Tangible & measurable
  – Insurable in some cases
  – Provides basis for prosecution and/or litigation

• Political costs:
  – Loss of integrity
  – Diminished public confidence
  – Can’t be measured, difficult to recover
  – Employee Morale…….
Profile of a fraud perpetrator…

- Male, but increasing percentage of females
  - Median loss is higher for males than females ($185,000 for males and $83,000 for females)

- Intelligent and in management
  - Managerial employees are 16 times more likely to commit fraud than non-managerial employees

- Married and under some type of significant stress

- Risk takers and not afraid to fail

- Rule breakers

- Long-time employees, hard working, rarely call in sick or take vacation

Source: “Fraud Perpetrator Profile: A Short Story” by Nick Brignola, CFE
Profile of a fraud perpetrator…

Tenure of Perpetrator – Median Loss

Median Loss

Tenure of Perpetrator

Source: Association of Certified Fraud Examiners, Report to the Nation on Occupational Fraud & Abuse 2014
Profile of an organization at risk...

- Less than 100 employees
- Management ignores irregularities
- High turnover with low morale
- Staff lacks training
- Trust placed in employees
- Employees have detailed knowledge of the accounting systems and their weaknesses
- Management subverts normal controls
- Management under PRESSURE
- Related Party Transactions
- Outdated or incomplete procedure manuals.

Source: “Fraud Perpetrator Profile: A Short Story” by Nick Brignola, CFE
What can Management do?

Corporate Culture – Tone at the Top
Tone at the top describes the ethical environment created in a company by leadership. Tone does trickle-down to employees. Four steps to creating the right tone:

1. Lead by example
2. Communicate & Train Employees
3. Institute an effective Whistleblower program
4. Reward ethical behavior

Minimize Opportunity – Strong Internal Controls
Overview of data analytics in the anti-fraud and fraud investigation context
Data Analytics in an Investigative Context

- What is Data Analytics (DA)?
- How is it employed in the internal audit / consultative environment?
- How can it be used as a tool in an investigation?
- Proactive versus reactive data analytics
- What are the advantages of the use of data analytics versus traditional forensic investigative techniques?
Understanding the Need for Data Analytics

• More data is stored electronically than ever:
  - Financial
  - Customer
  - Vendor
  - Marketing / Sales Leads
  - Communications (email, text, social media)

• Data analysis techniques and specialized software can identify red flags for fraud, and can analyze large sets of data rather than using statistical, random or judgmental sampling of transactions
What might we find with Data Analytics (DA)?

- Control gaps / failures
- Errors and inefficiencies
- Fraud or fraud risks

Proactive/detective data analytic purposes:

- Generally looking for previously unknown patterns indicative of fraud or loss
- Identification of high risk areas to enhance controls or concentrate further investigative efforts/action
- Can also be used to confirm suspected patterns and help determine root cause relationships
- Can be used to support an overall Fraud Risk Assessment and Fraud Management / Awareness Program

What is different with an investigations context?

- [Often] you know where to begin your focus
  - Process(es), patterns, specific accounts/vendors, etc.
- May analyze more detailed information, such as meta data, or larger populations of data (longer time periods)
- Heavier review of results, including comparing results to other publically available information (e.g., social media) or requesting information via subpoena
Fraud’s Increasing Trajectory

- Typically starts out small
- Increases in complexity and aggressiveness
- Often grows in magnitude and in number of participants
- Will rarely cease on its own
## Fraud Risks/Schemes in Common Processes

<table>
<thead>
<tr>
<th>Vendors / Accounts Payable (AP)</th>
<th>Employees / Payroll</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Conflict of interest / kickbacks</td>
<td>- Embezzlement/Theft</td>
</tr>
<tr>
<td>- Embezzlement/Theft</td>
<td>- Ghost employee (never or was previously employed)</td>
</tr>
<tr>
<td>- Fictitious/Ghost vendor</td>
<td>- Unauthorized or improper payroll payments</td>
</tr>
<tr>
<td>- False invoicing scheme</td>
<td>- Falsified or inflated hours or overtime</td>
</tr>
<tr>
<td>- Bid rigging</td>
<td>- Anti-corruption (in addition to Ghost employee risks)</td>
</tr>
<tr>
<td>- Anti-corruption</td>
<td>- Hiring unauthorized/illegal employees (incl. government)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Corporate Expenses/Purchase Card</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Embezzlement/Theft (personal expenses)</td>
<td></td>
</tr>
<tr>
<td>- Anti-corruption (entertaining or making payments to government officials)</td>
<td></td>
</tr>
</tbody>
</table>
Fraud Risks/Schemes in Common Processes

- Customers / Accounts Receivable
- Embezzlement/Theft
  - Lapping / Re-directing deposits
- Conflict of interest / kickbacks
- Earnings management (inflating assets / revenue)

- Manual Journal Entries (GL)
  - Earnings management, most typically:
    - Increase assets, revenue
    - Decrease liabilities, expense
    - Balance sheet gross-up
- Concealment of improper cash disbursements

Data mining or data analysis (often used interchangeably) can target specific activities or transactions that are at higher risk of fraud using indicators such as specific types of transactions, patterns within the data, or relationships between sets of data that should not exist.
Methodology for Performing Data Analytics

Business Environment
- Business & concerns
- Processes & systems

Scope
- Processes to analyze
- Data to collect (tables, time frame)
- Number and types of routines

Tool Selection and Determination of Risk Factors
- What tools will you use
- How will you determine high-risk records / criteria
Methodology for Performing Data Analytics

Load Data
- Import tables
- Quality checks

Process Data
- Run routines
- Quality check results

Results Review and Reporting of Risk Areas
- Review findings
- Report to stakeholders
Data Analysis Flow: Example

- **User Interface**
  - (Risk Scoring and Test Results)

- **Repository of Analytical / Forensic Procedures**
  - (Classified by Business Process)

- **Rules Engine**

- **Data Aggregator**

- **Data Loader**

- **Examples of Client Data**
  - (Multiple Sources such as SAP, Oracle, In-House, etc)
  - Vendor Master List
  - Employee Master List
  - Payments, Invoices, etc.

- **Public Information**
  - External Data Sources
Focus on High Risk and High Value Transactions

Frequency Anomalies

Inconsistency in Data Sets

High Risk & Value

Data Anomalies
Capability limitations of traditional data analytics methods and how to overcome
Ongoing Benefits of Routine DA Include…

- Identify compliance failures on a timely basis
- Continually evaluate control environment adequacy and effectiveness
- Mitigate control weaknesses
- Objective basis for quantifying system-wide risk
- Allocate limited resources efficiently
- Reduce cost by correcting errors
- Eliminate inefficiency and waste
- Uncover high risk relationships
- Improve existing internal audit protocols
- Assess compliance with regulatory environment
- Identify area of improvement for training and development, targeted and agency-wide
Current Challenges

- Increasingly Complex Regulatory Environment:
  - Foreign Corrupt Practices Act (FCPA) / Dodd-Frank Whistleblower
  - Sarbanes and Oxley

- Business processes and controls don’t operate perfectly

- Collusion is difficult to prove / uncover

- Compliance resources must be allocated efficiently

- Performance pressures may create unintended incentives to achieve metrics

- Obtaining a COMPLETE data set – from all available sources (oft missed examples may include data stored on smart phones, personal laptops, cloud-based environments)
Other Limitations and How to Overcome

- **Quality Assurance**
  - Data import issues
  - Complete population
  - All fields necessary / desired are not readily available (e.g., MCC Codes, purchasing warehouses, etc.)

- **Sampling vs. complete population**
  - Test 100% of population, when possible (Big Data)

- **Use of summary trends rather than transaction-level**
  - Frequencies
  - Time lines
  - Various other visualizations

- **Time consuming to repeat**
  - Scripts
  - Normalization

Involvement of IT Department, selected vendors (Financial institution), corroborating manual tests, and other techniques can help to resolve these issues.
The power of combining publicly available information and data visualization technology
Example: Public Information for Employee, Vendor Cross-check

- **Utilizing public information can tell you:**
  - If an address is invalid or high risk
  - A phone number is invalid or tied to a temporary address
  - An employee address or phone ties to a business
  - Employee SSN belongs to a deceased person
  - Address is a check cashing store
  - Whether an individual owns a business or certain types of property
  - Certain types of court case activities / charges
Potential Ghost Employee: Address is a Hotel, SSN Pattern or Other IDs are invalid for Active Payroll Employee
Visualization Tools

Benefits of visualizing results:

- Compelling way to tell a story – not just numbers
  - “A picture is worth a million words”
- Useful to risk management
- Dashboards add immediate understanding of data world working with
- Conflict results can be simplified
### Visualization Tools

#### Top 10 Users / Cardholders

<table>
<thead>
<tr>
<th>Description</th>
<th>Dollars Spent</th>
<th>Top Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERMIT OPERATIONS - Manager, CC&amp;O CC Mgmt, Water</td>
<td>$359,667.86</td>
<td>DCGOV DDOT PERMITS</td>
</tr>
<tr>
<td>Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executive Assistant I, ISF Fleet Management</td>
<td>$86,250.33</td>
<td>Aramark Uniform</td>
</tr>
<tr>
<td>Executive Assistant II, Finance &amp; Budget</td>
<td>$73,934.54</td>
<td>OEMSupplies</td>
</tr>
<tr>
<td>Secretary to the Board</td>
<td>$71,070.42</td>
<td>Staples</td>
</tr>
<tr>
<td>Manager, CC&amp;O CC Mgmt, Water Services</td>
<td>$63,590.36</td>
<td>DCGOV DDOT PERMITS</td>
</tr>
<tr>
<td>Senior Executive Assistant, OGM</td>
<td>$53,312.41</td>
<td>Howard University</td>
</tr>
<tr>
<td>Administrative Services Coordinator, Engineering &amp;</td>
<td>$50,994.10</td>
<td>Amazon</td>
</tr>
<tr>
<td>Technical Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executive Assistant II, OGM</td>
<td>$43,837.68</td>
<td>Amazon</td>
</tr>
<tr>
<td>Executive Assistant I, Engineering &amp; Technical Services</td>
<td>$43,009.11</td>
<td>U.S. Office Solutions</td>
</tr>
<tr>
<td>Executive Assistant II, Information Technologies</td>
<td>$39,171.63</td>
<td>Amazon</td>
</tr>
</tbody>
</table>

Source: Internal Audit Analysis from Citibank FY 2016 Data.

#### FY 2016 P Card Spending

- **Office Products**: 23%
- **Fleet Related**: 4%
- **Food and Catering**: 10%
- **IT**: 2%
- **Industrial**: 20%
- **Government, Special Purchases, Professional Memberships**: 32%
## Visualization Tools

<table>
<thead>
<tr>
<th>Vendor Name</th>
<th>Charge Amount</th>
<th>% of Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>THOMSON LEGAL &amp; REG</td>
<td>$ 526,085</td>
<td>3%</td>
</tr>
<tr>
<td>BUSINESS TRANSACTION</td>
<td>$ 476,708</td>
<td>2%</td>
</tr>
<tr>
<td>PODIATRY INSURANCE COMPANY</td>
<td>$ 359,568</td>
<td>2%</td>
</tr>
<tr>
<td>OFFICEMAX CONTRACT</td>
<td>$ 313,393</td>
<td>2%</td>
</tr>
<tr>
<td>MARK PAYPAL</td>
<td>$ 287,046</td>
<td>2%</td>
</tr>
<tr>
<td>SQUARE</td>
<td>$ 255,817</td>
<td>2%</td>
</tr>
<tr>
<td>AT&amp;T CONS CLARIFY MOBILITY</td>
<td>$ 246,713</td>
<td>2%</td>
</tr>
<tr>
<td>BDO USA</td>
<td>$ 237,000</td>
<td>1%</td>
</tr>
<tr>
<td>OUCPAYMENT/SPEEDPAY</td>
<td>$ 217,422</td>
<td>1%</td>
</tr>
<tr>
<td>SSG CATALOG</td>
<td>$ 210,918</td>
<td>1%</td>
</tr>
<tr>
<td>MATTHEW BENDER &amp; CO INC</td>
<td>$ 209,138</td>
<td>1%</td>
</tr>
<tr>
<td>AMERICAN AIRLINES E TKT</td>
<td>$ 207,019</td>
<td>1%</td>
</tr>
<tr>
<td>JETBLUE AIRWAYS</td>
<td>$ 158,804</td>
<td>1%</td>
</tr>
<tr>
<td>MALLAH, FURMAN &amp; COMPANY,</td>
<td>$ 155,791</td>
<td>1%</td>
</tr>
<tr>
<td>TROPHIES BY EDCO INC</td>
<td>$ 151,822</td>
<td>1%</td>
</tr>
<tr>
<td>DELTA AIR LINES</td>
<td>$ 148,695</td>
<td>1%</td>
</tr>
<tr>
<td>AMERICAN AIRLINES INC</td>
<td>$ 121,036</td>
<td>1%</td>
</tr>
<tr>
<td>COLLEGEBOARD SEARCH</td>
<td>$ 115,286</td>
<td>1%</td>
</tr>
<tr>
<td>PUFF N STUFF CATERING</td>
<td>$ 109,762</td>
<td>3%</td>
</tr>
<tr>
<td>OTHER/MISC</td>
<td>$ 108,481</td>
<td>2%</td>
</tr>
<tr>
<td>Remaining Named Suppliers</td>
<td>$ 14,243,617</td>
<td>75%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>$ 18,860,119</strong></td>
<td></td>
</tr>
</tbody>
</table>
Example of Risk Management Dashboard
Example of Vendor Risk Dashboard
Examples of Social Network Diagram to Visualize Shared Data Elements
Real world examples of indications of fraud identified using advanced data analytics, public information and visualization technology
Case Studies

Conflict of Interest:

- Test identified an employee with the same address as a contractor, but different phone number and last name
- Upon investigation, it was determined the contractor was the son of the employee, and the employee not only supervised the work, but also determined how much the contractor was paid
- Over $20,000 was paid to the contractor and the relationship was not disclosed on the vendor conflict forms (‘no relationships’ was checked by the employee)

Misappropriation of Assets / Altered Payee:

- Tests identified vendor bank account numbers that matched an employee's bank account numbers
- An Accounts Payable clerk used the vendor master change function to change the payable information to his own name during the check run and change it back once the run was completed
- The employee had collected several hundreds of thousands in diverted payments
Employee Expense Fraud:

- Whistleblower indicated suspect personal and false expense reimbursement requests from a senior executive
- Data analysis routines, coupled with timeline visualization, helped identify over $50,000 in inappropriate spend, including falsified receipts

Employee Fraud:

- Ghost Employees - Identified 21 terminated employees that received over $1 million in payroll payments
- Identified an employee whose SSN, according to public records, was issued prior to birth and belonged to a deceased individual. The employee was an active employee on payroll.
Case Studies

Payroll / Time Theft:

- Hotline caller anonymously reported 2nd-shift employee of leaving facility to attend night classes without clocking out, with knowledge of immediate supervisor
- Data analysis routines, cross referencing timesheet authorization by supervisor, building badge logs, and parking lot video surveillance (with assistance from Facilities department) determined that the allegation was substantiated and the employee and supervisor were subsequently terminated.

Inventory Fraud:

- Anonymous tip that surplus assets were being stolen from the warehouse, listed as retired / disposed and sold on e-Bay or Craigslist
- Cross referenced inventory results (Missing / Retired) assets to surplus sales / warehouse inventory results, disposition codes, to identify high risk transactions; performed public information search of online auction sites, serial number checks and identified over $25,000 in misappropriated assets.
Fraudulent Invoice Scam Example

• Bogus invoices sent from a company called “Scholastic School Supply”
  – Showed an amount due of $647.50 was due for math or art books that were not ordered or received
  – Payment addresses were mail drops

• This scam hit schools in 27+ states including Florida

• Reminder of importance to verify all bills before they are paid
Bogus Invoices

On a busy day, would you catch this as a fake?
Florida Middle School Fraud Scenario

**Ex-bookkeeper accused of embezzling more than $100,000 from Florida Middle School**

- Principal became concerned about negative balances in School-Wide Fundraiser general ledger project account.
- Bookkeeper made out checks to vendors and rewrote 110 checks to herself, stealing approximately $108,000.
- Bookkeeper altered Principals Reports and other documentation to hide the impact of the altered checks on funds performance.
- She altered Monies Collected Forms and stole approximately $124,000 in cash from deposits.
Auditor released June 9, 2017 indicates evidence of fraud and misspending on construction projects.

- Parents had been complaining for months about school improvement projects not getting done
- Bond money paid for a new multipurpose facility
- Construction company was paid $330,000 for 4 projects that have yet to start
- Board members will move to terminate the construction contract at the July 13 Board meeting
Detroit Public Schools Corruption Scheme

Feds arrested 12 principals, 1 administrator and 1 vendor in March 2016 for bribery/kickbacks of $1million

- School supplies vendor paid principals nearly $1 million for using his company
- Scheme occurred for 13 years, total payments to principals range from $4,000 to $324,000
- Charges stem from an audit that raised red flags for 1 of the principals and led to arrest
- Kickbacks were in the form of cash, giftcards, and payment to vendors to work on residences
Appendix:
Identity Verification through External Data Sources
## Vendor Verification – Public Data Sources – Summary of Results Found

### Vendor File Results

<table>
<thead>
<tr>
<th>Message or Driver</th>
<th>Count</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid Zip Code</td>
<td>15</td>
<td>1.34%</td>
</tr>
<tr>
<td>Zip is invalid.</td>
<td>2</td>
<td>0.18%</td>
</tr>
<tr>
<td>Probable Vacant Address</td>
<td>32</td>
<td>2.86%</td>
</tr>
<tr>
<td>Address is invalid</td>
<td>181</td>
<td>16.20%</td>
</tr>
<tr>
<td>AddressWatch: Address is Suspect</td>
<td>44</td>
<td>3.94%</td>
</tr>
<tr>
<td>Address is a Temporary Address</td>
<td>20</td>
<td>1.79%</td>
</tr>
<tr>
<td>Check cashing store address</td>
<td>2</td>
<td>0.18%</td>
</tr>
<tr>
<td>Address is Not Currently Receiving Delivery</td>
<td>30</td>
<td>2.69%</td>
</tr>
<tr>
<td>Address is Not Valid at Delivery Point</td>
<td>192</td>
<td>17.19%</td>
</tr>
<tr>
<td>Address Unit Number Missing</td>
<td>9</td>
<td>0.81%</td>
</tr>
<tr>
<td>Check cashing store address</td>
<td>2</td>
<td>0.18%</td>
</tr>
<tr>
<td>Unit Number Present but Not Verified</td>
<td>14</td>
<td>1.25%</td>
</tr>
<tr>
<td>Invalid Phone</td>
<td>91</td>
<td>8.15%</td>
</tr>
<tr>
<td>Phone reported only with different Address(es)</td>
<td>75</td>
<td>6.71%</td>
</tr>
<tr>
<td>Phone and Zip code mismatch</td>
<td>34</td>
<td>3.04%</td>
</tr>
<tr>
<td>Phone is Cellular or Mobile</td>
<td>92</td>
<td>8.24%</td>
</tr>
<tr>
<td>Phone listed to a Mail Delivery Location</td>
<td>9</td>
<td>0.81%</td>
</tr>
<tr>
<td>Phone listed to a Temporary address</td>
<td>7</td>
<td>0.63%</td>
</tr>
<tr>
<td>Phone listed to Prison</td>
<td>0</td>
<td>0.00%</td>
</tr>
</tbody>
</table>
# Employee Verification – Public Data Sources – Summary of Results Found

## Employee File Results

<table>
<thead>
<tr>
<th>Message or Driver</th>
<th>Count</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address is invalid</td>
<td>29</td>
<td>1.00%</td>
</tr>
<tr>
<td>Probable Vacant Address</td>
<td>31</td>
<td>1.07%</td>
</tr>
<tr>
<td>Address is a Business Address</td>
<td>34</td>
<td>1.17%</td>
</tr>
<tr>
<td>Address is a Mail Delivery Address</td>
<td>14</td>
<td>0.48%</td>
</tr>
<tr>
<td>Address is Not Currently Receiving Delivery</td>
<td>9</td>
<td>0.31%</td>
</tr>
<tr>
<td>Address is Not Valid at Delivery Point</td>
<td>75</td>
<td>2.62%</td>
</tr>
<tr>
<td>Address is a Temporary Address</td>
<td>2</td>
<td>0.07%</td>
</tr>
<tr>
<td>Address Unit Number Missing</td>
<td>41</td>
<td>1.41%</td>
</tr>
<tr>
<td>Unit Number Present but Not Verified</td>
<td>28</td>
<td>0.97%</td>
</tr>
<tr>
<td>AddressWatch: Address is suspect</td>
<td>9</td>
<td>0.31%</td>
</tr>
<tr>
<td>Check cashing store address</td>
<td>1</td>
<td>0.03%</td>
</tr>
<tr>
<td>Name not reported at Address</td>
<td>47</td>
<td>1.65%</td>
</tr>
<tr>
<td>Known fraud address</td>
<td>1</td>
<td>0.03%</td>
</tr>
<tr>
<td>Invalid Phone</td>
<td>7</td>
<td>0.24%</td>
</tr>
<tr>
<td>No Name or Address reported with Phone</td>
<td>89</td>
<td>3.07%</td>
</tr>
<tr>
<td>Phone listed to a Temporary address</td>
<td>1</td>
<td>0.03%</td>
</tr>
<tr>
<td>Phone and Zip code mismatch</td>
<td>13</td>
<td>0.52%</td>
</tr>
<tr>
<td>Phone listed to Business</td>
<td>7</td>
<td>0.26%</td>
</tr>
<tr>
<td>Phone reported only with different Address(es)</td>
<td>48</td>
<td>1.66%</td>
</tr>
<tr>
<td>Phone reported only with different First name(s)</td>
<td>164</td>
<td>5.66%</td>
</tr>
<tr>
<td>Phone reported only with different Last name(s)</td>
<td>60</td>
<td>2.07%</td>
</tr>
<tr>
<td>Potentially unlisted &amp; unverified Phone</td>
<td>10</td>
<td>0.35%</td>
</tr>
<tr>
<td>Social Issued After Age 18</td>
<td>129</td>
<td>4.45%</td>
</tr>
<tr>
<td>Social Issued Before DOB</td>
<td>5</td>
<td>0.17%</td>
</tr>
<tr>
<td>Social Issued in Last Three Years</td>
<td>9</td>
<td>0.21%</td>
</tr>
<tr>
<td>Deceased Identity Found with Full Name Match</td>
<td>5</td>
<td>0.16%</td>
</tr>
<tr>
<td>Social Invalid</td>
<td>4</td>
<td>0.14%</td>
</tr>
<tr>
<td>Social field contains an ITIN</td>
<td>1</td>
<td>0.03%</td>
</tr>
<tr>
<td>Social Not Recognized Before Randomization Date</td>
<td>48</td>
<td>1.66%</td>
</tr>
</tbody>
</table>
QUESTIONS AND ANSWERS?
Don’t let it happen to you……..