LexisNexis

RISK SOLUTIONS
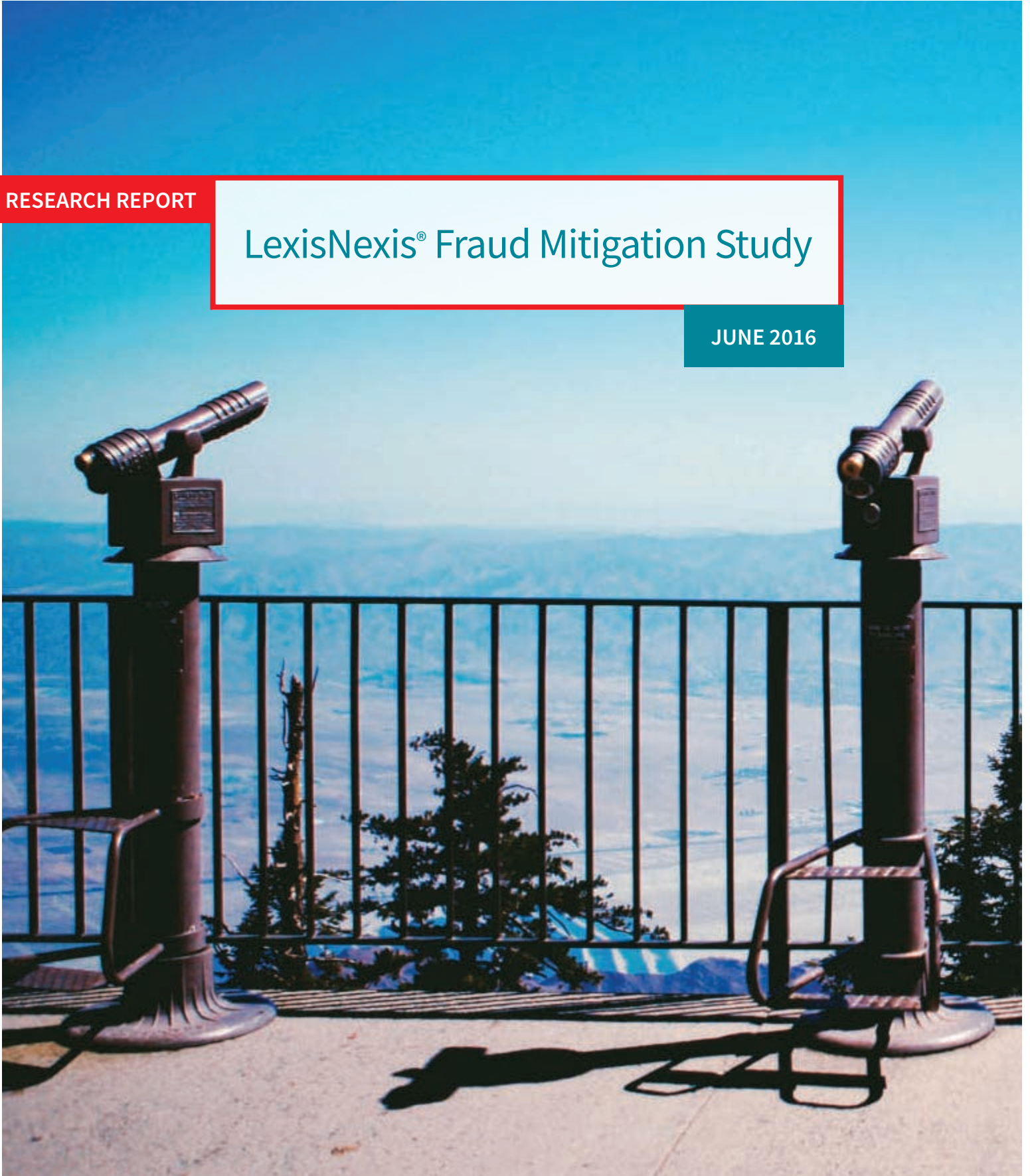
LexisNexis® Fraud Mitigation Study

JUNE 2016

Executive summary

LexisNexis® Risk Solutions administered a national online survey of 800 fraud mitigation professionals from the following industries:

- Insurance
- Retail
- Government
- Financial services
- Health care
- Communications

The survey was conducted in two phases and closed in April of 2016. It has a margin of error of +/- 3 points (at the 95 percent confidence level). LexisNexis was not identified as the sponsor of the research.

Goals of research

LexisNexis Risk Solutions commissioned the Fraud Mitigation Study to understand fraud that touches multiple industries. For example, in an insurance investigation, is there evidence that the potential perpetrator also committed benefits fraud or financial fraud, etc.? In addition to looking at the impact of fraud that crosses industries, the study explored the extent to which fraud mitigation professionals rely on external data and analytics solutions to help with their fraud mitigation programs.

Findings related to multiple industry fraud

Evidence of cross-industry fraud exists in a majority of cases. Moreover, these cases have moderate-to-high financial repercussions. Fraud mitigation professionals are interested in leveraging data about fraud from other organizations, especially within their own industry, but also across industries. Respondents also see value in the concept of a universal and consistent way to talk about fraud across all industries. Insurance organizations see the most cross-industry fraud and believe it impacts their own investigations the most, especially compared to government and health care. Insurance and financial services organizations place the most value in accessing outside data, and in establishing a common language for fraud across industries.

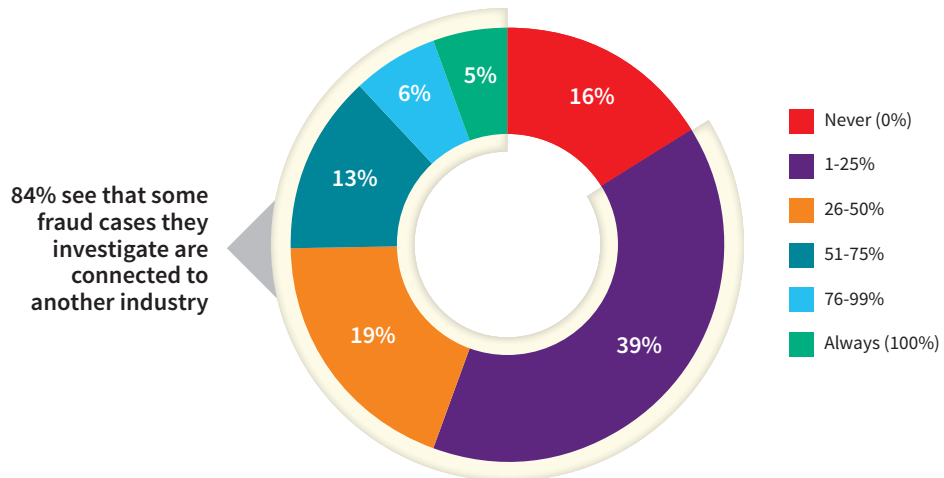## Findings related to the use of data analytics solutions in fraud prevention

About 75 percent of those surveyed are using both external data and analytics solutions in their fraud mitigation programs, most often driven by the desire for compliance and accuracy. For analytics, most fraud mitigation professionals are primarily using automated business rules systems, behavioral analytics, predictive modeling and ad hoc database searches.

Other key findings

Fraud schemes of greatest concern vary by industry. Organizations are most concerned about identity theft (particularly within financial services and retail), hacking (especially within communications), fraud involving employees (government's top concern), and claims fraud (insurance and health care). If given additional budget for their fraud programs, respondents say they would spend it on technological systems, followed by training, data, process improvements, staff and then analytics.

Part I: Trends Related to Cross-Industry Data

Percentage of fraud cases connected to another industry*

84% see that some fraud cases they investigate are connected to another industry

Pie chart values: 16%, 39%, 19%, 13%, 6%, 5%

Legend:
- Never (0%)
- 1-25%
- 26-50%
- 51-75%
- 76-99%
- Always (100%)

Industry-specific findings:
Insurance organizations most often say that all their cases are cross-industry (12%). Government (22%) and health care (21%) most often say their cases are never cross-industry.

Q.S2.2: Approximately what percent of the time would you say that the fraud cases you've encountered or investigated also turn out to be connected to industries outside of your own? Based to those giving a scale response: 705

Financial impact

76% of cross-industry fraud cases have moderate-to-high impact on organizations, with more than half causing extreme impact

Bar chart: 53% | 23% | 24%

Legend:
- Extreme or high impact
- Moderate impact
- Little to no impact

Industry-specific findings:
Insurance respondents reported that 61% of cross-industry fraud cases had an extreme-to-high impact, compared to government (48%) and health care (46%).

Q.S2.2a: On a scale of 1-5, with 1 being 'no financial impact' and 5 being 'extremely high financial impact,' please rate the financial impact that these cases have on your organization. Based to those giving a scale response: 572

*The percentages listed in this report may not total 100 percent due to rounding.

Impact of cross-industry fraud vs. within-industry fraud

63% see cross-industry fraud creating at least an equal impact, if not a greater impact, as within-industry fraud

29%	34%	37%

- ■ Larger impact
- ■ Equal impact
- ■ Smaller impact
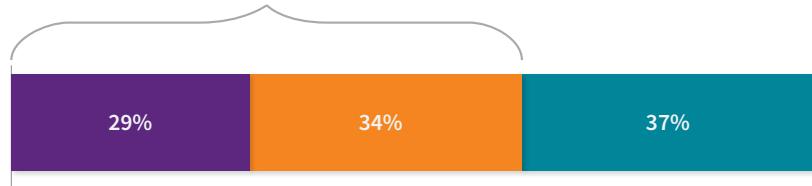
Industry-specific findings:

Government (46%) and health care (45%) professionals most often report that cross-industry fraud cases have a smaller impact than fraud cases in their own industry.

Q.S2.2b: Do you feel these cross-industry fraud cases have a larger, smaller or equal impact on your organization compared to cases that are solely within your industry (within-industry fraud)? Based to those giving a scale response: 273

Value of access to data for known fraud activities

84% believe access to within-industry fraud data would be valuable

Within Industry

57%	27%	16%

Industry-specific findings:

Insurance (68%) and financial services (64%) most often report that within-industry data would be very valuable or valuable.

75% believe that cross-industry fraud data would be valuable

Outside Industry

42%	33%	25%

- ■ Very valuable or valuable
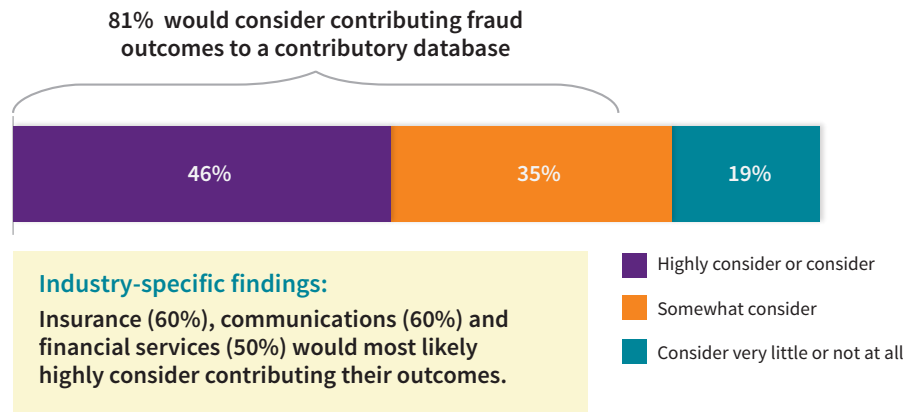- ■ Moderately valuable
- ■ Not very or not at all valuable

Q.S2.3: On a scale of 1-5, with 1 being 'not at all valuable' and 5 being 'very valuable,' what value would you place on having on-demand access to data about known fraud activities, events, persons or other attributes (address, e-mail, phone number, etc.) A: From other companies/agencies within your industry? B: From companies/agencies outside of your industry? Base: 800

Value of universal fraud descriptors

89% believe it would be valuable to develop universal fraud descriptors

53%	36%	12%

■ Very valuable or valuable

■ Somewhat valuable

■ Not very or not at all valuable

Industry-specific findings:

Insurance (63%) and financial services (61%) most often report that universal descriptors would be very valuable or valuable.
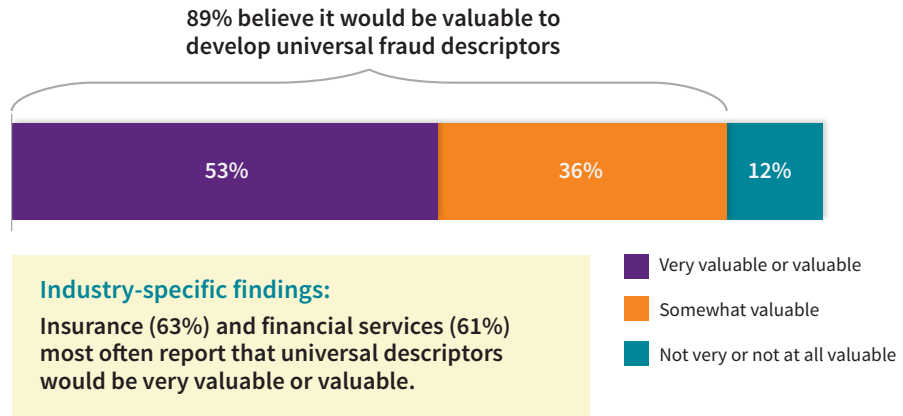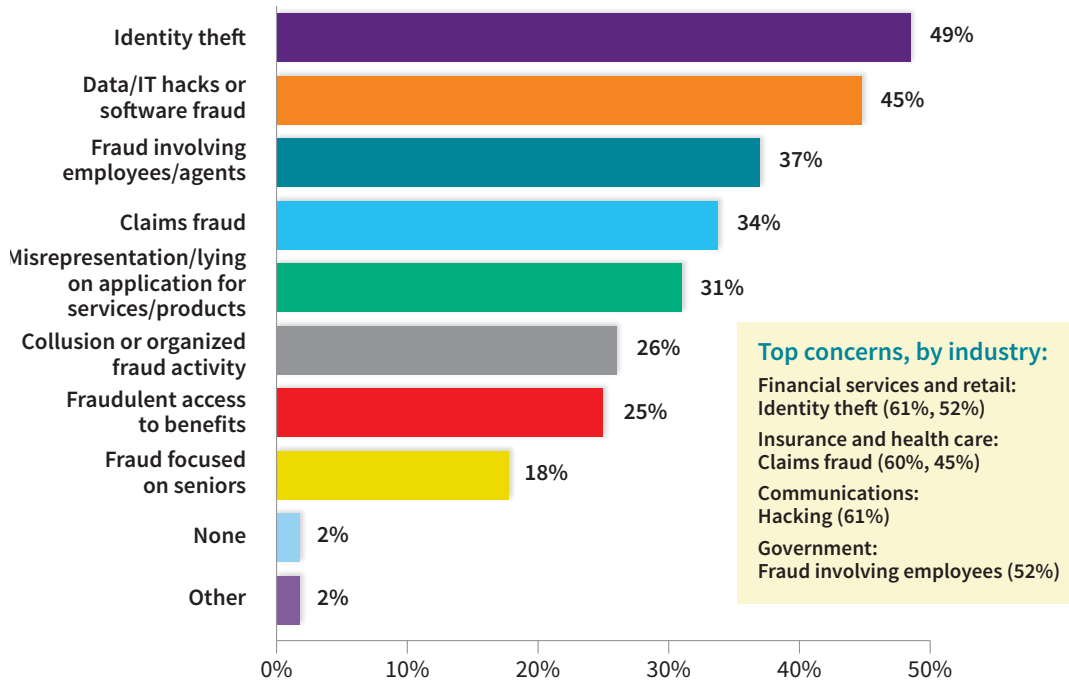
Q.S2.4: On a scale of 1-5, with 1 being 'not at all valuable' and 5 being ' very valuable,' what value would you place on establishing common, general ways of describing fraud that are universal across industries? For comparison or point of reference, think of the Standard Violation Codes used by the auto insurance industry to describe motor vehicle record violations, or the Current Procedural Terminology (CPT®) codes used by the health care industry. Base: 800

Likelihood to contribute fraud outcomes to contributory database

81% would consider contributing fraud outcomes to a contributory database

46%	35%	19%

■ Highly consider or consider

■ Somewhat consider

■ Consider very little or not at all

Industry-specific findings:

Insurance (60%), communications (60%) and financial services (50%) would most likely highly consider contributing their outcomes.
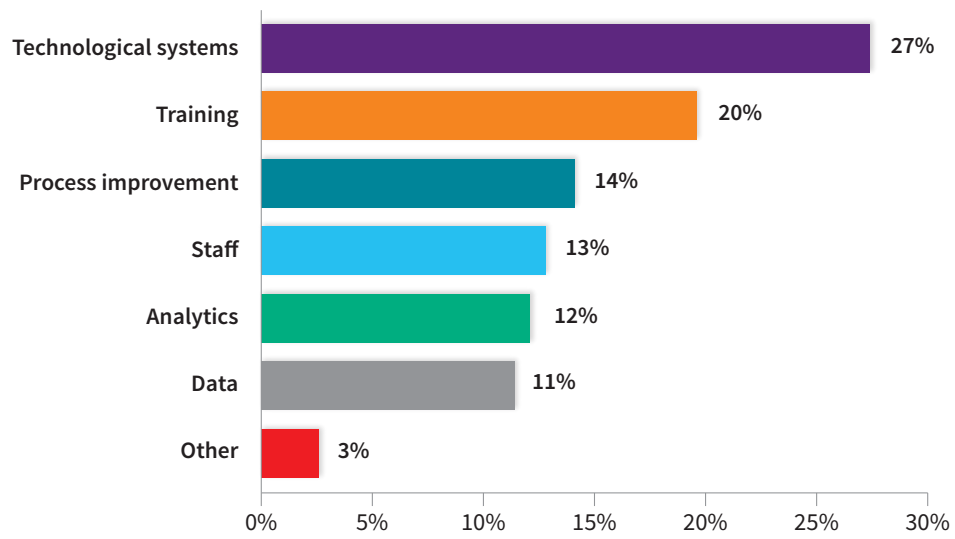
Q.S2.7: On a scale of 1-5 with 1 being 'not at all consider' and 5 being 'highly consider,' how much would you consider contributing the outcomes of your fraud investigations into a centralized solution if it meant that you would receive outcomes data back from other contributors across industries? Base: 400. Asked in Wave 2 only

Fraud schemes of greatest concern

Scheme	Percentage
Identity theft	49%
Data/IT hacks or software fraud	45%
Fraud involving employees/agents	37%
Claims fraud	34%
Misrepresentation/lying on application for services/products	31%
Collusion or organized fraud activity	26%
Fraudulent access to benefits	25%
Fraud focused on seniors	18%
None	2%
Other	2%

Top concerns, by industry:

Financial services and retail: Identity theft (61%, 52%)

Insurance and health care: Claims fraud (60%, 45%)

Communications: Hacking (61%)
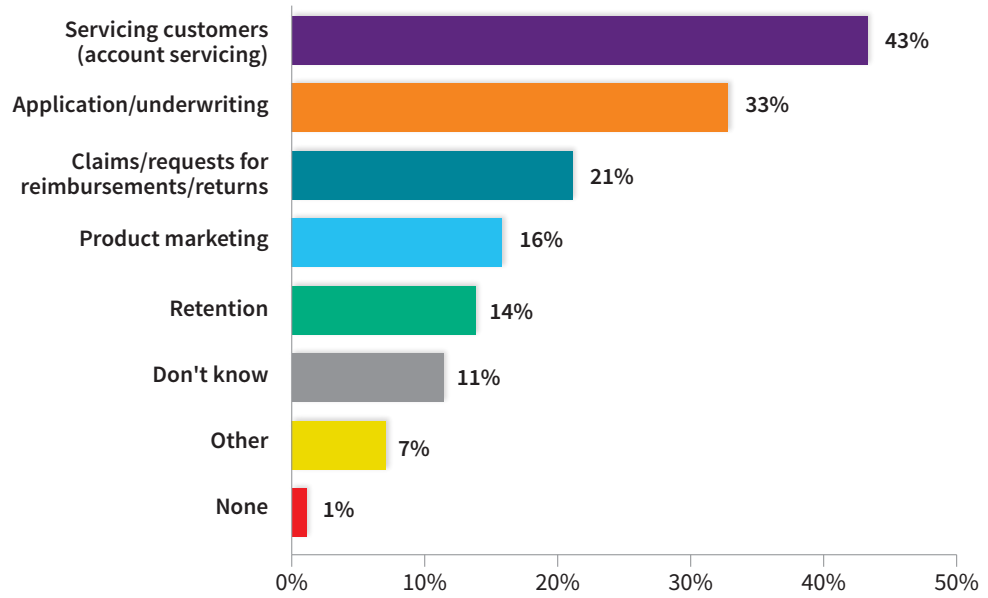
Government: Fraud involving employees (52%)

Q.S1.4: Which of the following fraud schemes is your organization highly concerned with? You can select multiple responses if applicable. Base: 400. Asked in Wave 2 only

Fraud mitigation spending priorities

Priority	Percentage
Technological systems	27%
Training	20%
Process improvement	14%
Staff	13%
Analytics	12%
Data	11%
Other	3%

Q.S1.5: If you had extra money to spend that would help you fight fraud more effectively, what would you spend it on first? Base: 800

Areas of fraud
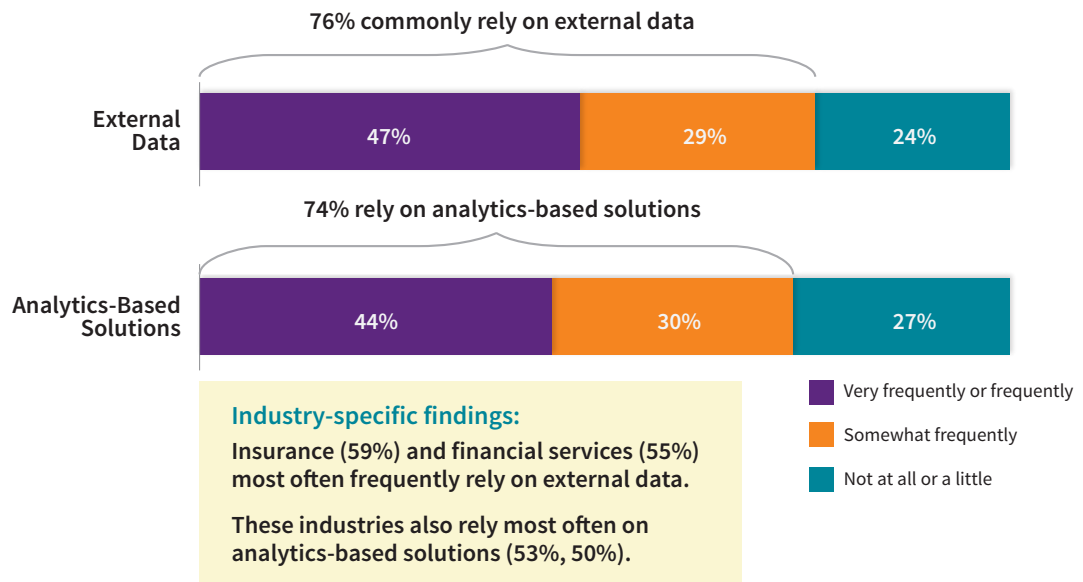

Area	Percentage
Servicing customers (account servicing)	43%
Application/underwriting	33%
Claims/requests for reimbursements/returns	21%
Product marketing	16%
Retention	14%
Don't know	11%
Other	7%
None	1%

Q.S2.1: In which of the following areas of your customer interactions do you see fraud?
Please check all that apply. Base: 800

Frequency of external data and analytics-based solution used for fraud mitigation

76% commonly rely on external data

| External Data | 47% | 29% | 24% |

74% rely on analytics-based solutions

| Analytics-Based Solutions | 44% | 30% | 27% |

■ Very frequently or frequently
■ Somewhat frequently
■ Not at all or a little

Industry-specific findings:

Insurance (59%) and financial services (55%) most often frequently rely on external data.

These industries also rely most often on analytics-based solutions (53%, 50%).

Q.S1.1: On a scale of 1-5, with 1 being 'not at all' and 5 being 'very frequently,' to what extent does your team rely on external data for fraud detection and mitigation?

Q.S1.2: On a scale of 1-5, with 1 being 'not at all' and 5 being 'very frequently,' to what extent does your team rely on analytics-based solutions for fraud detection and mitigation? Base: 800

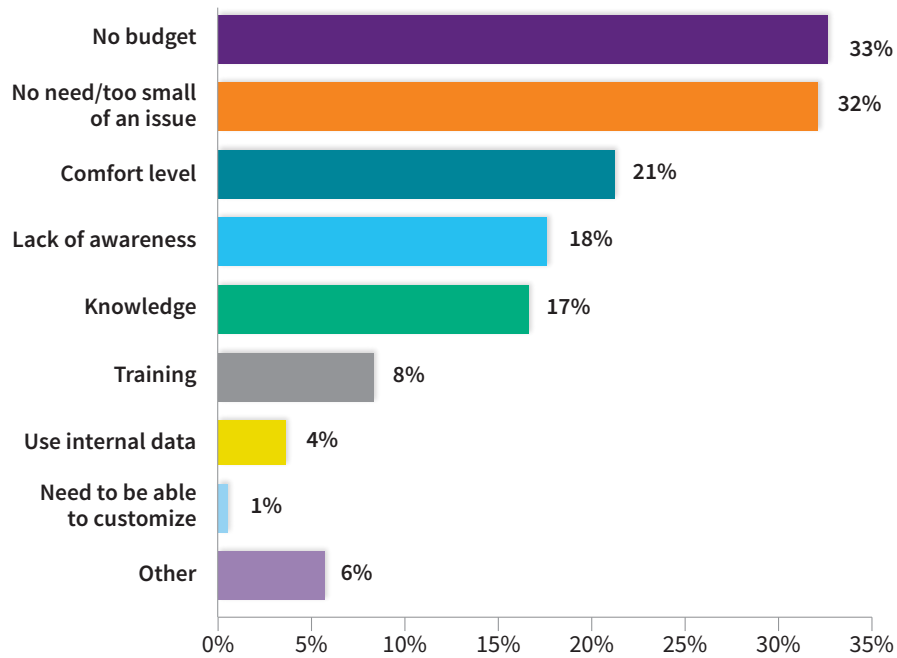### Drivers of external data use to improve fraud detection and mitigation

Driver	Percentage
Compliance	66%
Accuracy	56%
Industry best practice	46%
Effectiveness	46%
Speed	39%
Other	2%
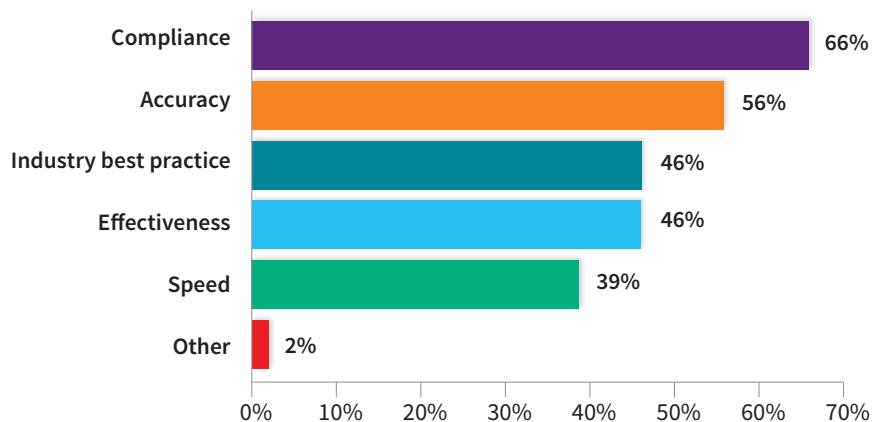
Industry-specific findings:

Financial services (77%), insurance (71%) and health care (69%) most often cite compliance as their number one reason for using external data.

Communications (62%) and retail (62%) most often cite accuracy as their number one reason.
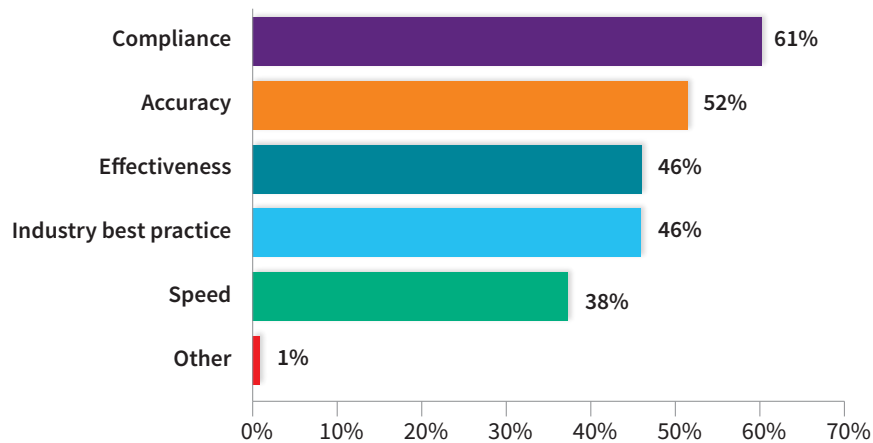
Q.S1.1a: What within your organization drives the need to use external data to improve fraud detection and mitigation? Please check all that apply. Base: 607. Asked to those rating Q.S1.1 as 3, 4 or 5.

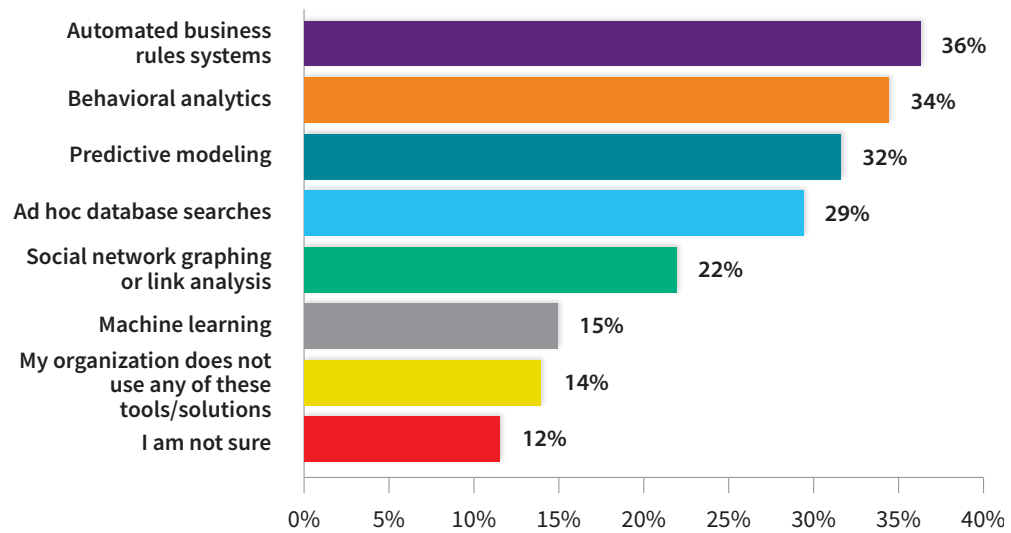## Reasons for not using external data for fraud detection and mitigation

Reason	Percentage
No budget	33%
No need/too small of an issue	32%
Comfort level	21%
Lack of awareness	18%
Knowledge	17%
Training	8%
Use internal data	4%
Need to be able to customize	1%
Other	6%

Q.S1.1b: Why is your organization not using external data for fraud detection and mitigation? Please check all that apply. Base: 193. Asked to those rating Q.S1.1 as 1 or 2.

Drivers of analytics-based solutions to improve fraud detection and mitigation

Driver	Percentage
Compliance	61%
Accuracy	52%
Effectiveness	46%
Industry best practice	46%
Speed	38%
Other	1%

Industry-specific findings:
Compliance is more commonly a driver for analytics-based solutions for insurance (68%), government (67%) and financial services (69%) than for communications (49%) and retail (47%).

Q.S1.2a: What within your organization drives the need to use analytics-based solutions to improve fraud detection and mitigation? Please check all that apply. Base: 588. Asked to those rating Q.S1.2 as 3, 4 or 5.
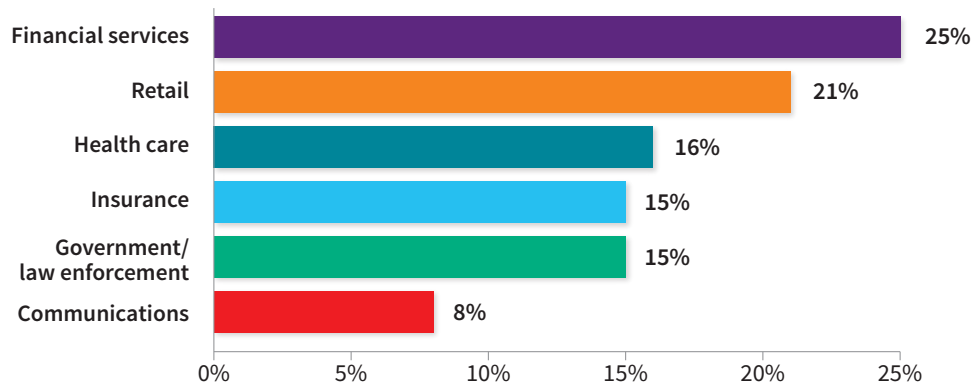
Reasons for not using analytics-based solutions for fraud detection and mitigation

Reason	Percentage
No need/too small of an issue	34%
No budget	33%
Lack of awareness	25%
Knowledge	17%
Comfort level	16%
Training	10%
Difficult to implement into review process	4%
Use internal software	2%
Unsure/not sure what covers	1%
Other	3%

Industry-specific findings:

Health care professionals were most likely to mention lack of awareness (32%) and comfort level (29%) as reasons for not using analytics-based solutions for fraud detection and mitigation.

Q.S1.2b: Why is your organization not using analytics-based solutions for fraud detection and mitigation? Please check all that apply. Base: 212. Asked to those rating Q.S1.2 as 1 or 2.

Most-used analytics-based solutions

Solution	Percentage
Automated business rules systems	36%
Behavioral analytics	34%
Predictive modeling	32%
Ad hoc database searches	29%
Social network graphing or link analysis	22%
Machine learning	15%
My organization does not use any of these tools/solutions	14%
I am not sure	12%

Q.S1.3: Which of the following represent the type(s) of analytics-based solutions that your organization has used in its fraud mitigation efforts? Please select all that apply. Base: 800

Representatives from each of our key vertical industries were surveyed

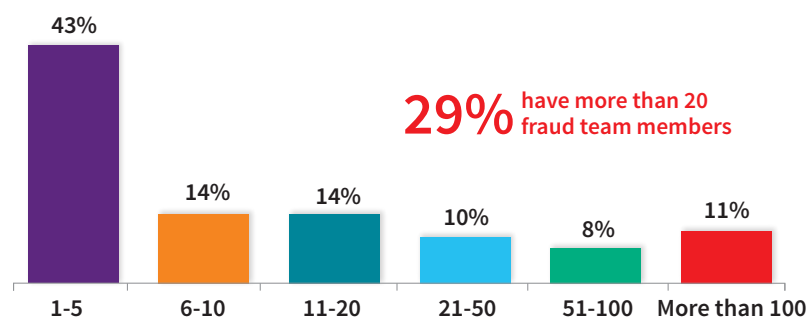| Industry	Percentage
Financial services	25%
Retail	21%
Health care	16%
Insurance	15%
Government/law enforcement	15%
Communications	8%

Q.A: Which of these industries are you currently employed in? Base: 800

Level of involvement in fraud mitigation

| Level	Percentage
Direct involvement in cases	50%
Oversight with some direct involvement in cases	32%
Oversight of fraud mitigation program with no direct involvement	18%

82% have direct involvement in fraud mitigation
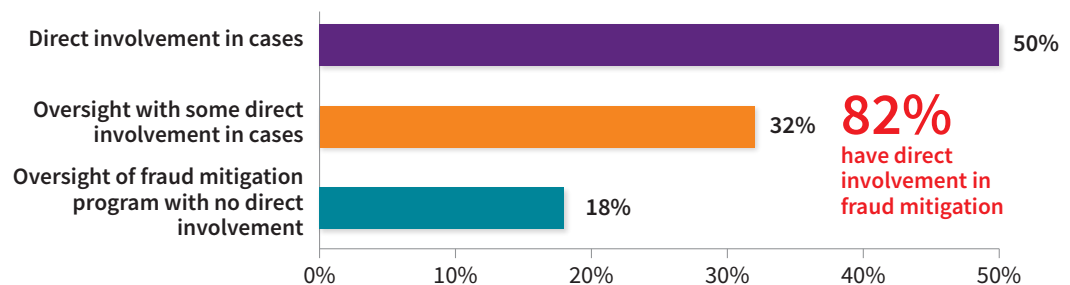
Q.B: What level of responsibility best describes your role related to fraud mitigation within your organization? Base: 800

Fraud team size

Size	Percentage
1-5	43%
6-10	14%
11-20	14%
21-50	10%
51-100	8%
More than 100	11%

29% have more than 20 fraud team members

Q.S3.4: Size of organization's fraud team (number of people)? Based to those giving a scale response: 749

Annual spending on data and analytics vendors

52% $500,000 or less
20% $501,000 – $1 million
28% More than $1 million
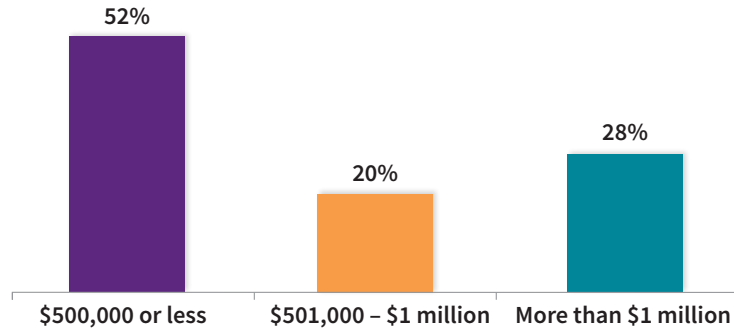
Q.S3.3: Amount your organization spends on fraud mitigation data and analytics vendors annually? Based to those giving a scale response: 675

Region

Northeast   23%
Midwest   21%
Southeast   18%
West   18%
Mid-Atlantic 10%
Southwest   10%
Other   1%

0%   5%   10%   15%   20%   25%
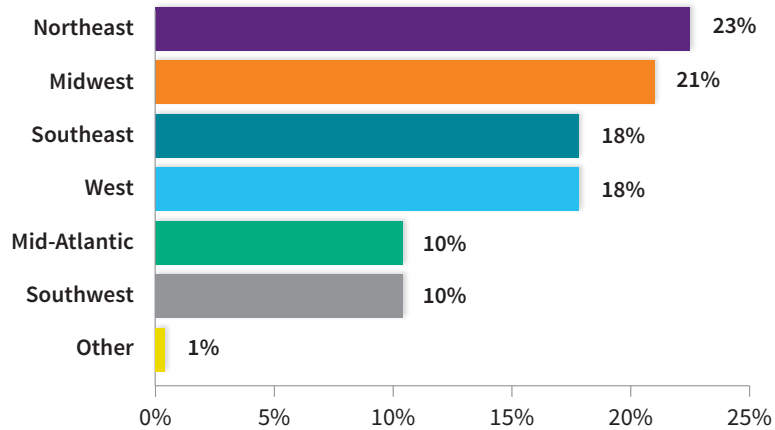
Q.S3.1: Region of country where you are located. Base: 800

Level in company

Analyst   3%
Manager   32%
Director   24%
VP or higher   37%
Other   4%

40%
30%
20%
10%
0%
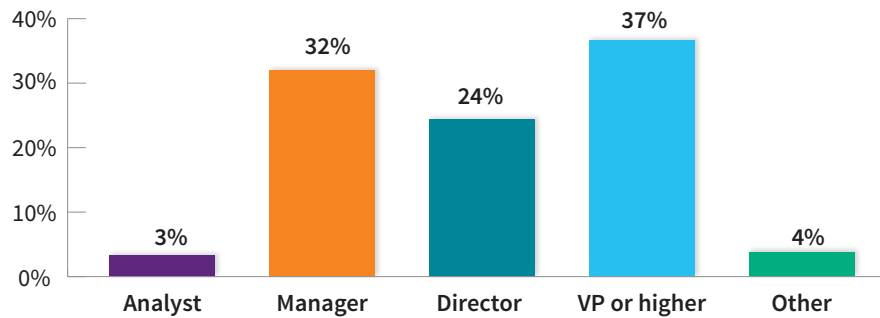
Q.S3.2: Your level within company. Base: 800

Company size

Less than 100	46%
100 – 1,000	28%
More than 1,000	27%
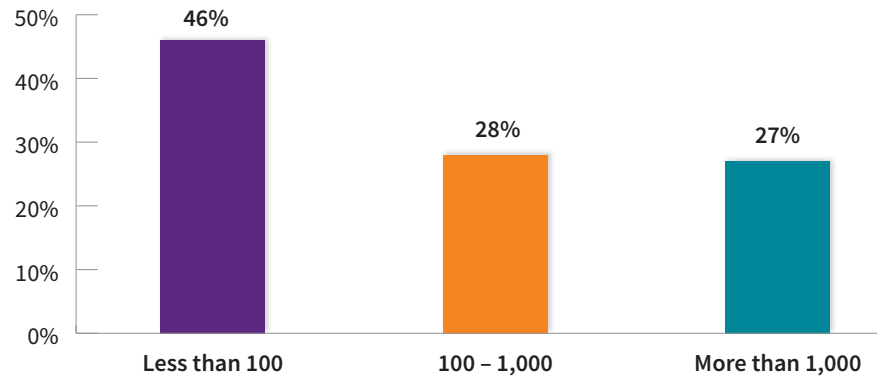
Q.S3.7: Company size (from sample). Based to those giving a scale response: 428

Lines of insurance supported

Personal lines (auto, home, etc.)	73%
Commercial lines (auto, property, general liability, etc.)	55%
Life insurance	47%
Workers' compensation insurance	38%
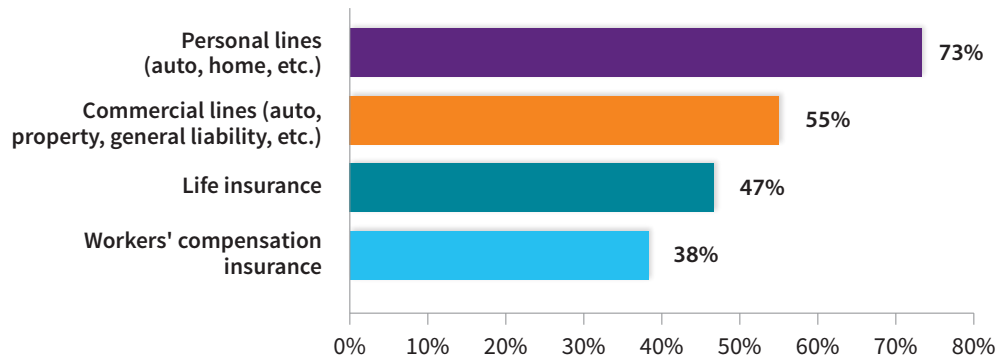
Q.AI: Which of the following best describes the line(s) of insurance you support at your company? You can select multiple areas if needed. Asked of insurance respondents in Wave 2. Base: 60

Type of health care organization

Commercial/private	84%
Government/public	16%
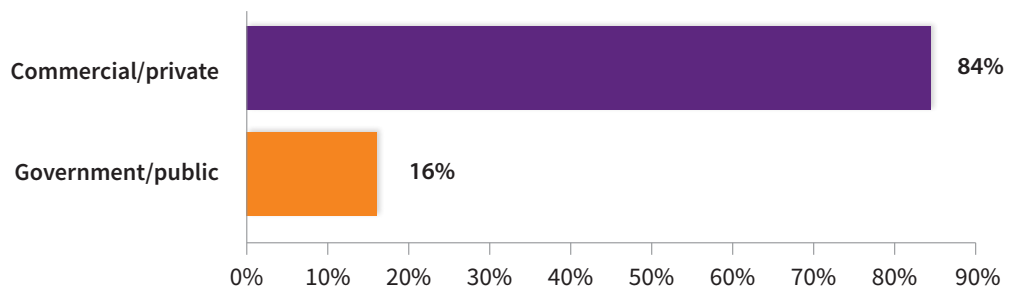
Q.AH: Would your organization best be described as a commercial/private health care company or a government/public agency? Asked of health care respondents in Wave 2. Base: 62

Area of government

Category	Value
Health and Human Services	32%
Regulatory and Administration	27%
Public Safety/Law Enforcement	19%
Tax and Revenue/Collections	6%
Other	16%

(Horizontal axis: 0% to 35%)
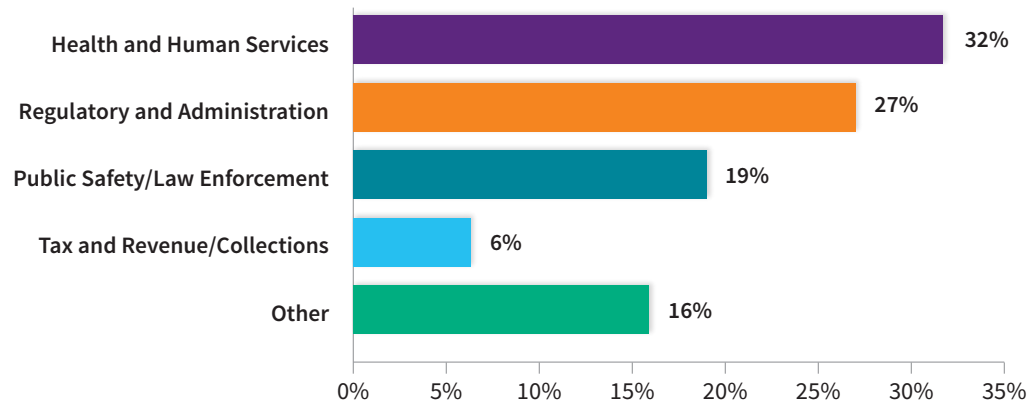
Q.AG1: Which of the following best describes the broad area of government you work within?
Asked of government respondents in Wave 2. Base: 63

Level of government

Category	Value
Local	48%
State	33%
Federal	19%

(Horizontal axis: 0% to 50%)
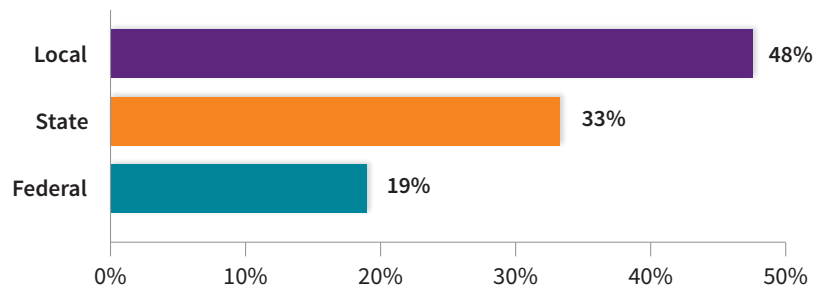
Q.AG2: Which of the following best describes the level of government you work within?
Asked of government respondents in Wave 2. Base: 63

LexisNexis®
Fraud Defense
Network

**For more information about the LexisNexis® Fraud Mitigation Study,
visit lexisnexis.com/fraudstudy or call 844.AX.FRAUD (844.293.7283)**

LexisNexis®
RISK SOLUTIONS