LexisNexis®
RISK SOLUTIONS

LexisNexis® Risk Solutions
Fraud Mitigation Study: 2017

SEPTEMBER 2017

LexisNexis®
RISK SOLUTIONS

Executive summary

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

- Insurance
- Retail
- Government
- Financial Services
- Healthcare
- Communications

The survey closed in June 2017, and has a margin of error of +/- three points (at the 95% confidence level). LexisNexis was not identified as the sponsor of the research.

Goals of research

LexisNexis® Risk Solutions commissioned its annual Fraud Mitigation Study to gauge trends and patterns related to fraud within several different industry sectors and government. Objectives of the 2017 study were to:

1) Determine the extent to which fraud extends into more than one industry. For example, in an insurance investigation, evidence may exist that the potential perpetrator also committed benefits fraud, financial fraud, etc.

2) Examine trends related to different types of fraud, including fraud resulting from stolen identities.

3) Explore 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

Over the past three years, our research has found that substantial levels of cross-industry fraud exist within our target industry sectors. Moreover, these cases have moderate-to-high financial repercussions. Fraud mitigation professionals are increasingly seeing the value of having fraud data from other organizations, especially within their own industry. Respondents additionally see increasing value in participating in a cross-industry contributory database for known fraud. Insurance organizations see the most cross-industry fraud and believe it impacts their own investigations the most, especially compared to respondents from government and retail organizations. Fraud mitigation professionals from insurance and financial services organizations place the most value in accessing outside data.

Findings related to fraud trends, identity fraud and online transactions

Fraud from stolen identities or cyber attacks/hacking were the types of fraud most concerning to fraud mitigation professionals. Moreover, as 60% of organizations have moved more of their transactions online over the past three years, there are greater concerns about identity fraud within online transactions versus within offline transactions (telephone, mail, in-person).

The majority of organizations have also taken additional steps to protect customers from identity fraud in the past year, such as implementing additional identity verification processes that customers must complete, conducting audits of their security systems, and increasing use of data analytics for earlier detection of fraud. These additional precautions are also consistent with the finding that organizations are currently spending more resources to identify/block suspicious transactions (42%) than in expediting safe transactions (28%). It remains to be seen how these trends are impacting the customer experience.
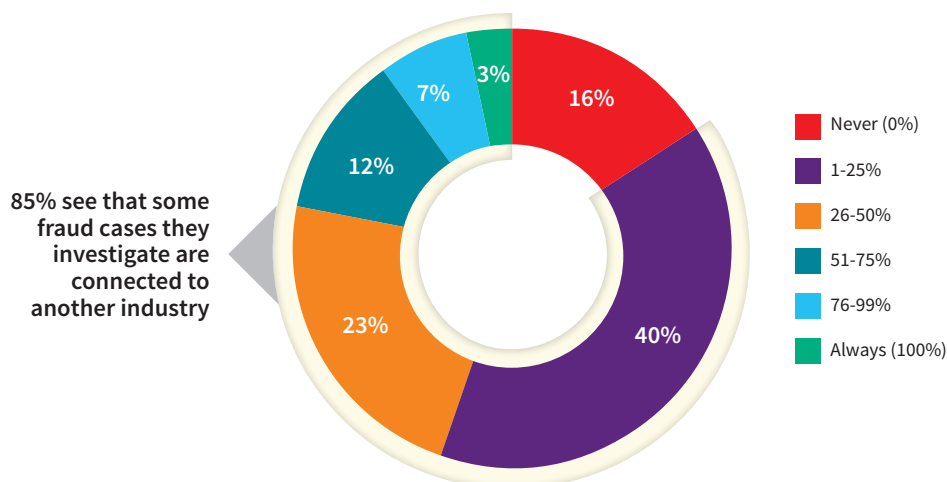
To fight against fraud, organizations spend the most on technological systems, followed by staff (especially within government) and training (healthcare), and most fraudulent transactions (37%) are associated with claims or requests for reimbursement, followed by account or customer service-related transactions (34%).

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

More than three quarters of those surveyed are using both external data and analytics solutions in their fraud mitigation programs, with reliance on external data increasing in 2017 to 79% (vs. 73% in 2015/2016 waves). For analytics, fraud mitigation professionals are primarily using behavioral analytics and predictive modeling, representing a slight shift from previous years where respondents also favored automated business rules. The change may be reflective of increasing sophistication in fraud mitigation methodologies.

Percentage of fraud cases connected to another industry*

85% see that some fraud cases they investigate are connected to another industry

Legend:
- Never (0%) — 16%
- 1-25% — 40%
- 26-50% — 23%
- 51-75% — 12%
- 76-99% — 7%
- Always (100%) — 3%

Industry-specific findings:
Retail (24%) and healthcare (18%) 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: 681

Financial impact

78% of cross-industry fraud cases have moderate-to-high impact on organizations, with almost half causing extreme impact

| 48% | 30% | 22% |

Legend:
- Extreme or high impact
- Moderate impact
- Little to no impact
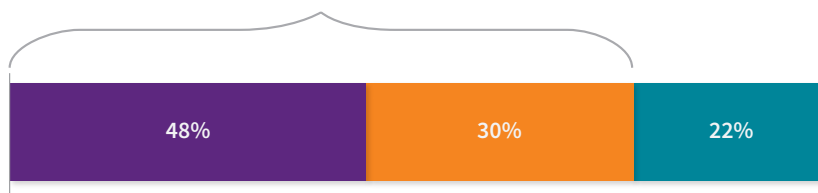
Industry-specific findings:
Insurance respondents reported that 50% of cross-industry fraud cases had an extreme-to-high impact, compared to retail (42%).

Communications reports the lowest impact of cross-industry fraud cases (31% low impact).

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

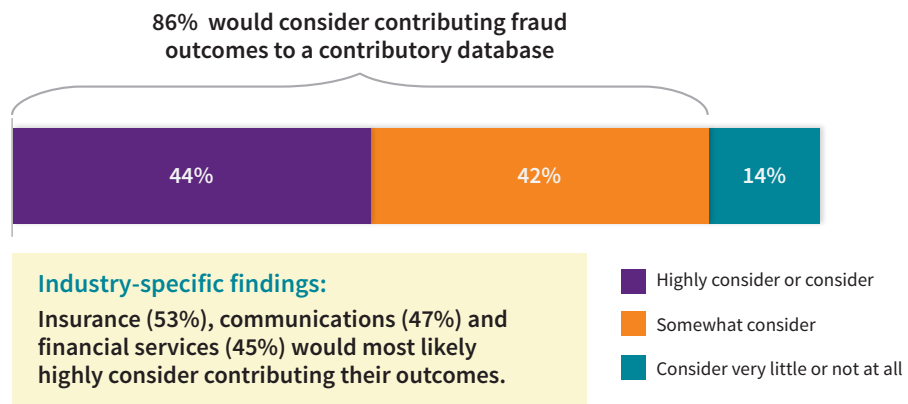*The percentages listed in this report may not total 100 percent due to rounding.

Value of access to data for known fraud activities

87% believe access to <u>within-industry</u> fraud data would be valuable

Within Industry		
55%	32%	13%

80% believe that <u>cross-industry</u> fraud data would be valuable

Outside Industry		
44%	36%	20%

Industry-specific findings:

Insurance (53%) and financial services (43%) most often report that outside-industry data would be very valuable or valuable.

- ■ 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
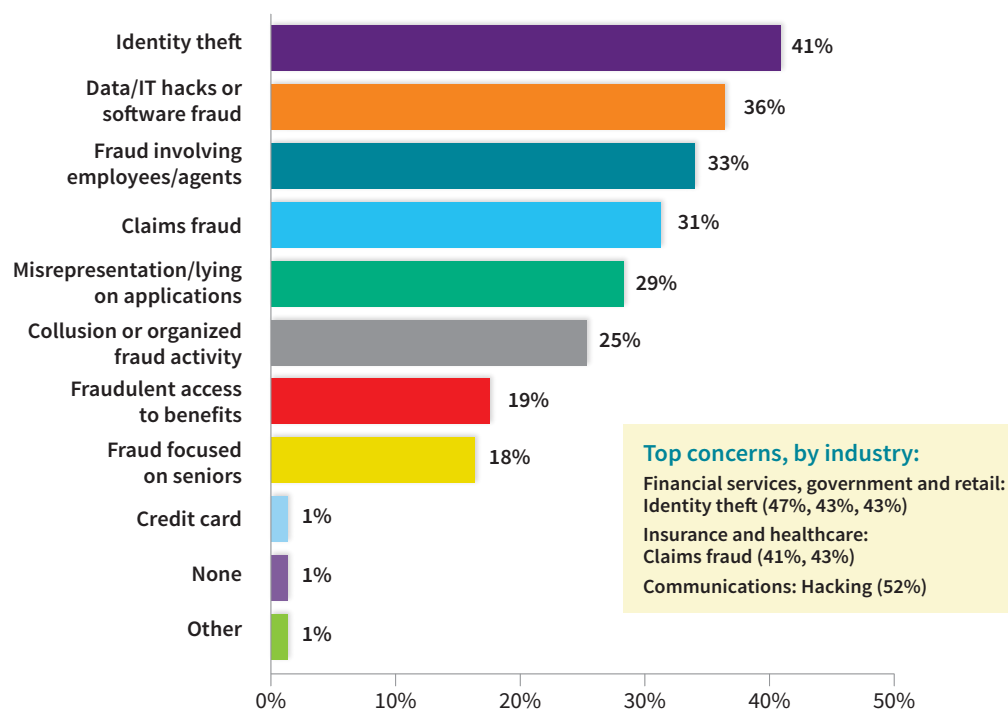
Likelihood to contribute fraud outcomes to contributory database

86% would consider contributing fraud outcomes to a contributory database

44%	42%	14%

Industry-specific findings:

Insurance (53%), communications (47%) and financial services (45%) would most likely highly consider contributing their outcomes.

- ■ Highly consider or consider
- ■ Somewhat consider
- ■ Consider very little or not at all

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: 800
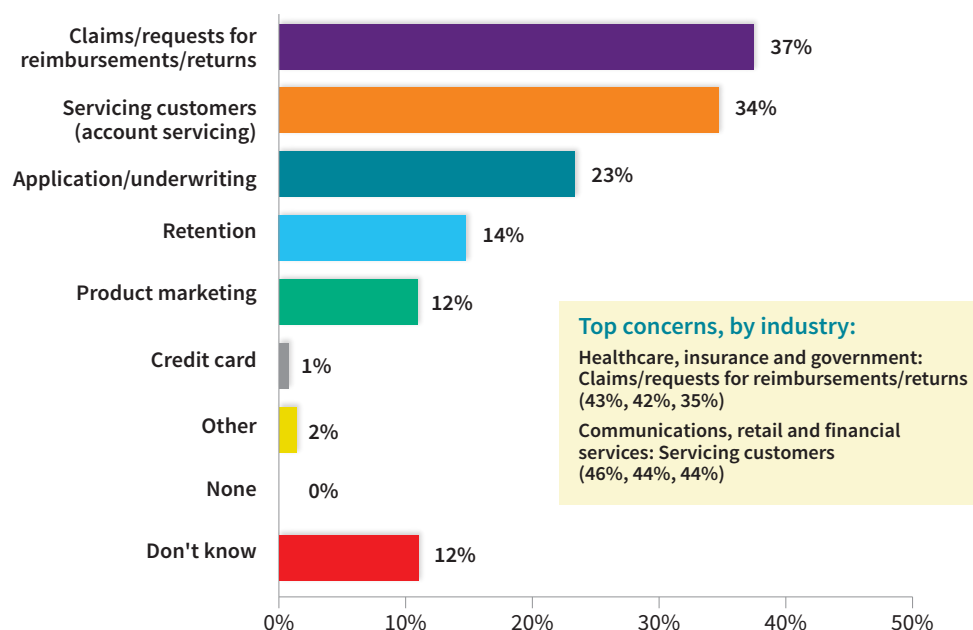
Fraud schemes of greatest concern

Category	%
Identity theft	41%
Data/IT hacks or software fraud	36%
Fraud involving employees/agents	33%
Claims fraud	31%
Misrepresentation/lying on applications	29%
Collusion or organized fraud activity	25%
Fraudulent access to benefits	19%
Fraud focused on seniors	18%
Credit card	1%
None	1%
Other	1%

Top concerns, by industry:
Financial services, government and retail:
Identity theft (47%, 43%, 43%)
Insurance and healthcare:
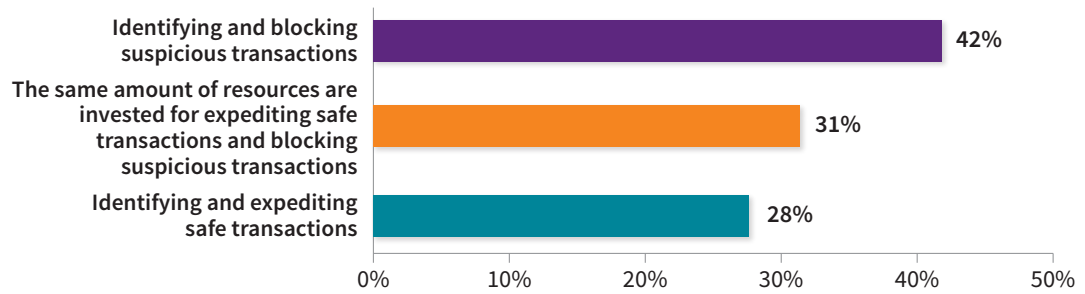Claims fraud (41%, 43%)
Communications: Hacking (52%)

Q.S1.4: Which of the following fraud schemes is your organization highly concerned with?
You can select multiple responses if applicable. Base: 800

Areas of fraud in customer interactions

Category	%
Claims/requests for reimbursements/returns	37%
Servicing customers (account servicing)	34%
Application/underwriting	23%
Retention	14%
Product marketing	12%
Credit card	1%
Other	2%
None	0%
Don't know	12%

Top concerns, by industry:
Healthcare, insurance and government:
Claims/requests for reimbursements/returns
(43%, 42%, 35%)
Communications, retail and financial
services: Servicing customers
(46%, 44%, 44%)

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

## Main organizational resource investments

Category	Percentage
Identifying and blocking suspicious transactions	42%
The same amount of resources are invested for expediting safe transactions and blocking suspicious transactions	31%
Identifying and expediting safe transactions	28%

Industry-specific findings:

Government (50%) and communications (49%) are most likely to invest in blocking suspicious transactions.

Insurance (37%) and healthcare (32%) verticals are most likely to invest in expediting safe transactions.

Q.S2.8: Does your organization currently invest more resources (time and budget) on…
Base: 800. Not asked in Waves 1 and 2.

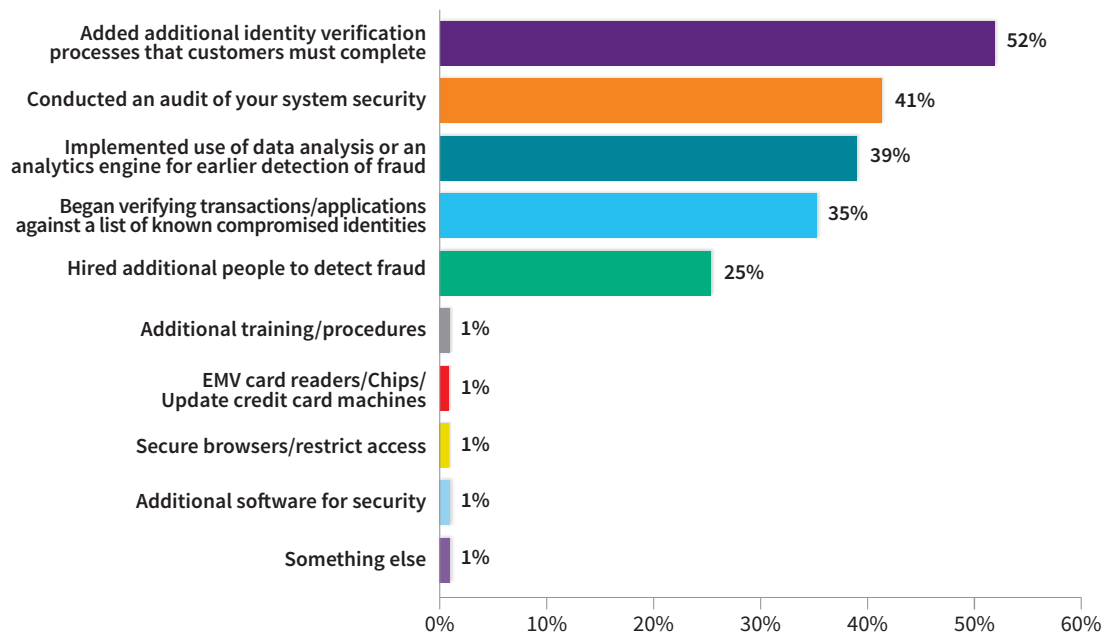## New organizational steps taken to protect customers from identity fraud

Response	Percentage
Yes	60%
No	27%
Don't know	13%
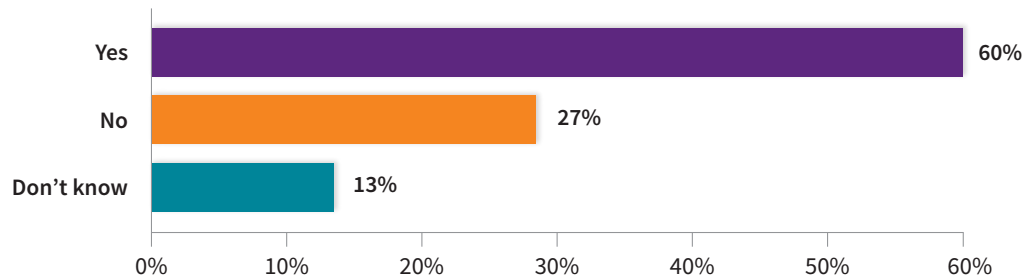
Industry-specific findings:

Financial services (65%) and insurance (62%) are most likely to have taken new steps to mitigate identity fraud.

Q.S2.11: In the past year, has your organization taken new or additional steps to protect customers from identity fraud? Base: 800. Not asked in Waves 1 and 2.

Additional steps taken to combat identity fraud

Step	Percentage
Added additional identity verification processes that customers must complete	52%
Conducted an audit of your system security	41%
Implemented use of data analysis or an analytics engine for earlier detection of fraud	39%
Began verifying transactions/applications against a list of known compromised identities	35%
Hired additional people to detect fraud	25%
Additional training/procedures	1%
EMV card readers/Chips/Update credit card machines	1%
Secure browsers/restrict access	1%
Additional software for security	1%
Something else	1%

Q.S2.12: What additional steps has your organization taken in the past year to protect customers from identity fraud? Base: 480. Not asked in Waves 1 and 2.

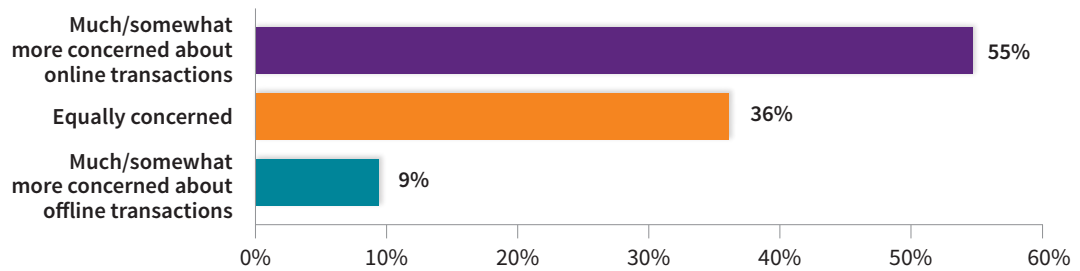## Organizational transaction movement online

Response	Percentage
Yes	60%
No	31%
Don't know	9%
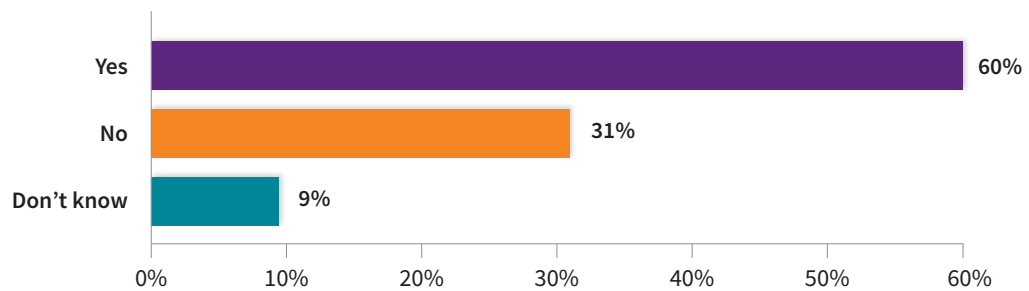
Industry-specific findings:
Communications (64%) and insurance (63%) respondents most often answer 'Yes.'
Retail (39%) and healthcare (34%) respondents most often answer 'No.'

Q.S2.9: Have more of your organization's transactions and services moved online over the past 3 years? Base: 800. Not asked in Waves 1 and 2.

Online versus offline identity fraud concern

Much/somewhat more concerned about online transactions — 55%

Equally concerned — 36%

Much/somewhat more concerned about offline transactions — 9%

(x-axis: 0% 10% 20% 30% 40% 50% 60%)

Industry-specific findings:

Insurance (63%), communications (61%) and financial services (59%) express the most concern with online transaction fraud.

Retail (12%), government (12%) and healthcare (11%) express more concern with offline fraud.

Q.S2.10: How concerned about identity fraud are you for online transactions versus for offline interactions (in-person, telephone, mail, etc.)? Base: 800. Not asked in Waves 1 and 2.
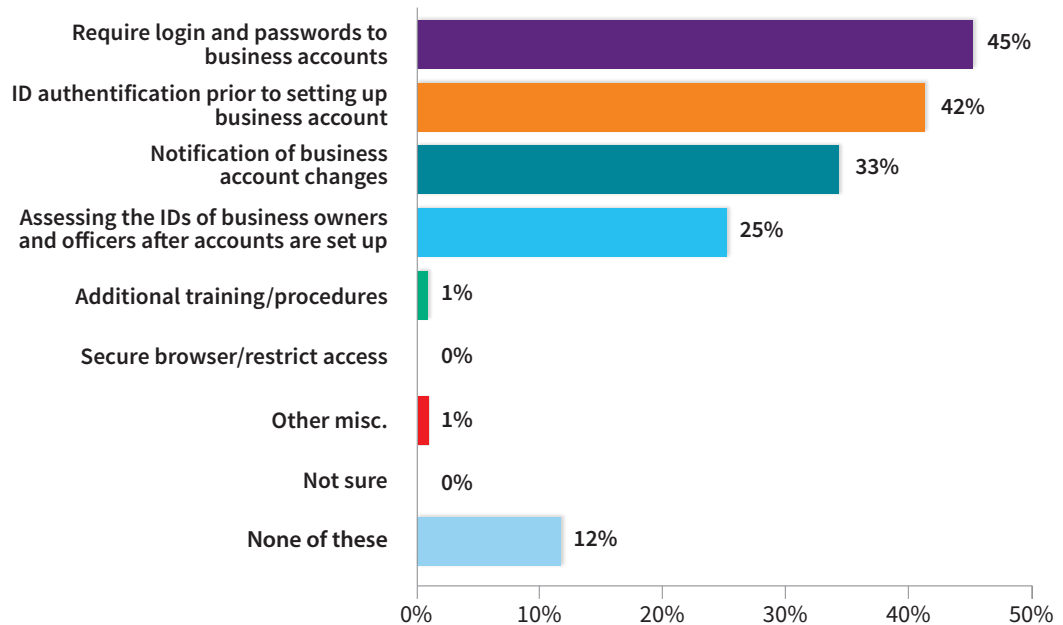
Business identity fraud across business accounts

Yes — 35%

No — 65%

(x-axis: 0% 10% 20% 30% 40% 50% 60% 70%)
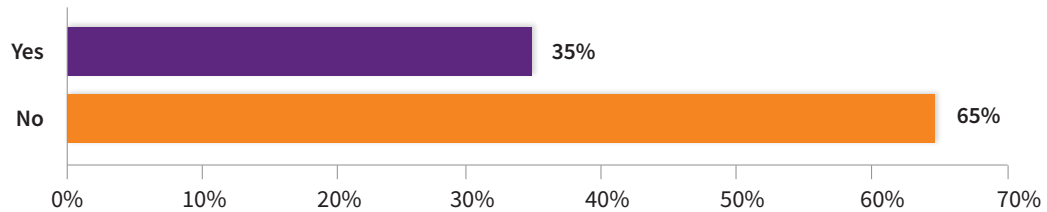
Industry-specific findings:

Insurance (50%) and financial services (42%) are most likely to have seen business fraud in the past year.

Retail (20%) is least likely to have seen business fraud.

Q.S2.13: In the past year, has your organization seen business identity fraud (criminals taking over the identity of a business) occur among your business accounts? Base: 669. Based to those who have business accounts. Not asked in Waves 1 and 2.
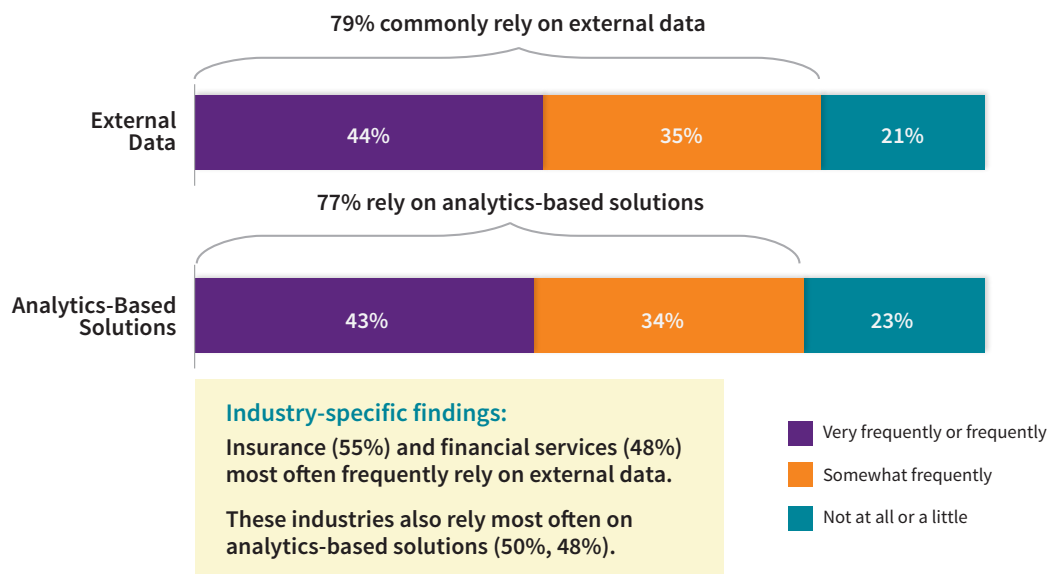
Additional steps taken to combat business identity fraud

Category	Percentage
Require login and passwords to business accounts	45%
ID authentification prior to setting up business account	42%
Notification of business account changes	33%
Assessing the IDs of business owners and officers after accounts are set up	25%
Additional training/procedures	1%
Secure browser/restrict access	0%
Other misc.	1%
Not sure	0%
None of these	12%

Q.S2.14: Which of the following have you done to prevent business identity fraud?
Base: 669. Not asked in Waves 1 and 2.

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

79% commonly rely on external data

External Data	44%	35%	21%

77% rely on analytics-based solutions

Analytics-Based Solutions	43%	34%	23%

Legend:
- ■ Very frequently or frequently
- ■ Somewhat frequently
- ■ Not at all or a little

Industry-specific findings:

Insurance (55%) and financial services (48%) most often frequently rely on external data.

These industries also rely most often on analytics-based solutions (50%, 48%).

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?
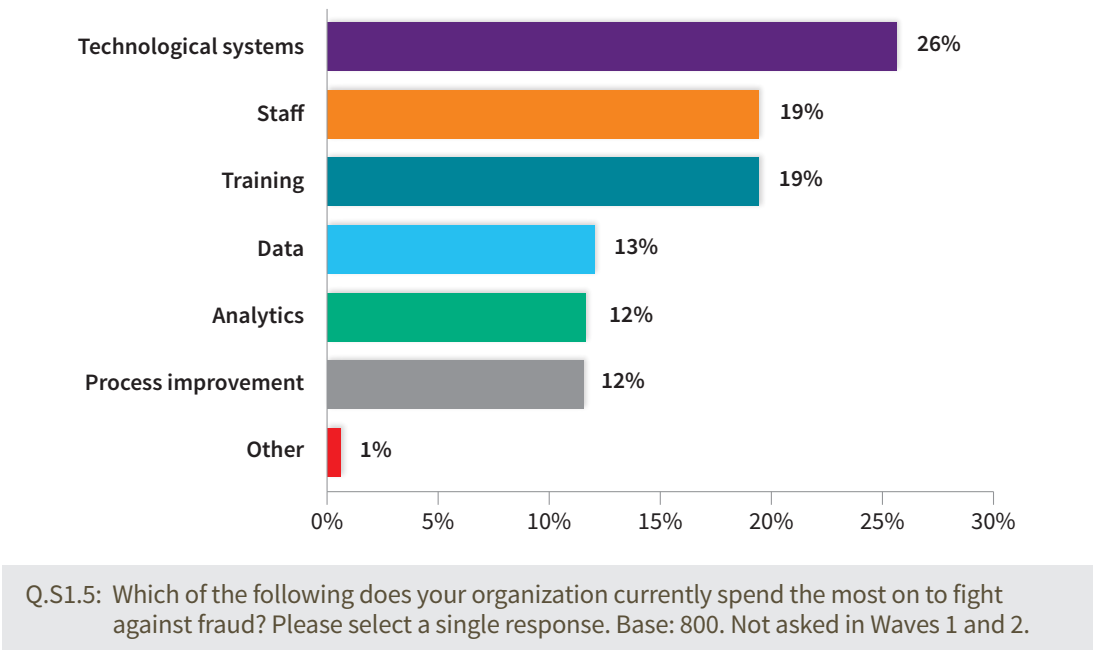Base: 800

Most-used analytics-based solutions

Solution	Percentage
Behavioral analytics	32%
Predictive modeling	27%
Automated business rules systems	25%
Ad hoc database searches	24%
Social network graphing or link analysis	21%
I am not sure	17%
Machine learning	14%
My organization does not use any of these tools/solutions	12%
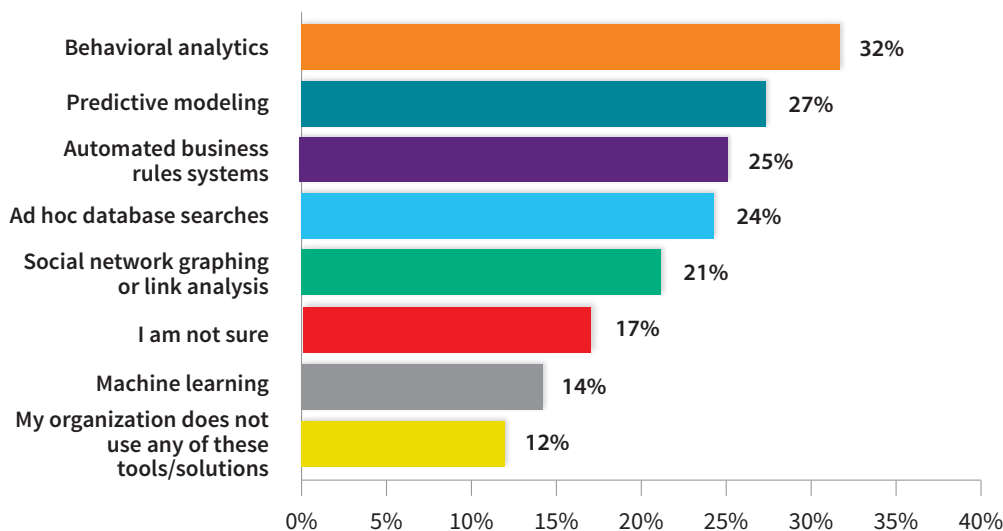
Q.S1.3: Which of the following represent the type(s) of analytics-based solutions that your organization has used in its fraud mitigation efforts? Please select all that apply.
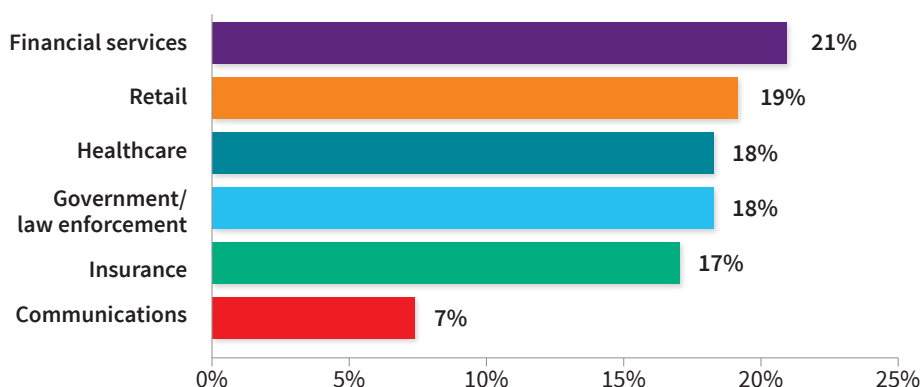Base: 800

Fraud mitigation spending priorities

Category	Percentage
Technological systems	26%
Staff	19%
Training	19%
Data	13%
Analytics	12%
Process improvement	12%
Other	1%

Q.S1.5: Which of the following does your organization currently spend the most on to fight against fraud? Please select a single response. Base: 800. Not asked in Waves 1 and 2.

Appendix 1: Basic Firmographics

Representatives from six industries were surveyed

Industry	Percentage
Financial services	21%
Retail	19%
Healthcare	18%
Government/ law enforcement	18%
Insurance	17%
Communications	7%

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	44%
Oversight with some direct involvement in cases	36%
Oversight of fraud mitigation program with no direct involvement	20%

80% 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	32%
6-10	18%
11-20	17%
21-50	12%
51-100	8%
More than 100	14%

34% have more than 20 fraud team members
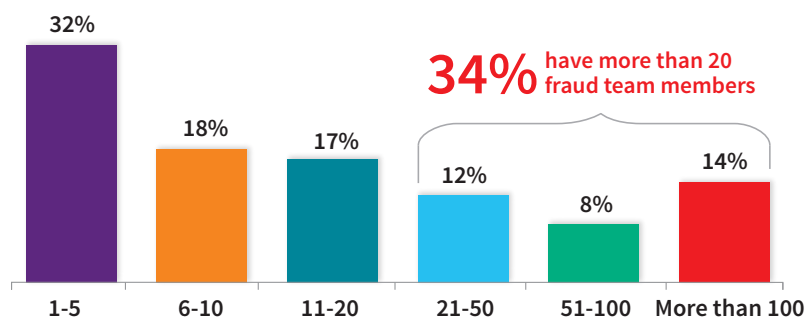
Q.S3.4: Size of organization's fraud team (number of people)? Based to those giving a scale response: 718

Annual spending on data and analytics vendors
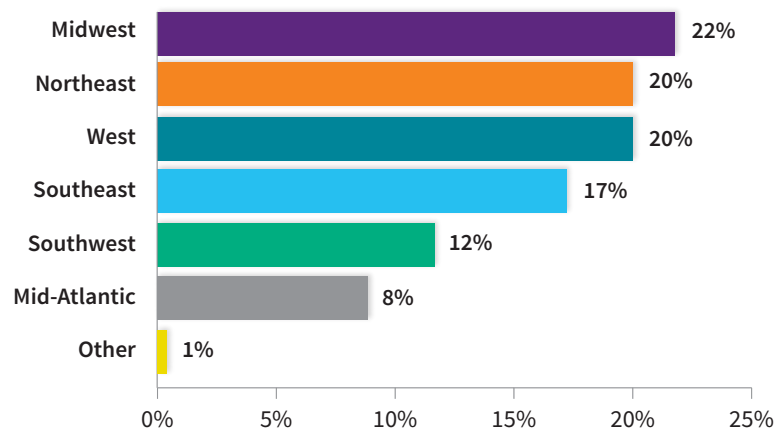
54% spend $500M+

$500,000 or less	$501,000 – $1 million	More than $1 million
45%	19%	35%

Region

Region	%
Midwest	22%
Northeast	20%
West	20%
Southeast	17%
Southwest	12%
Mid-Atlantic	8%
Other	1%

Level in company

Analyst	Manager	Director	VP or higher	Other
10%	34%	22%	27%	8%
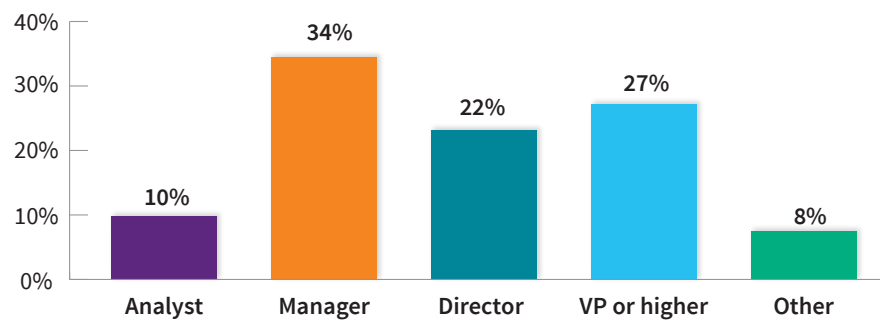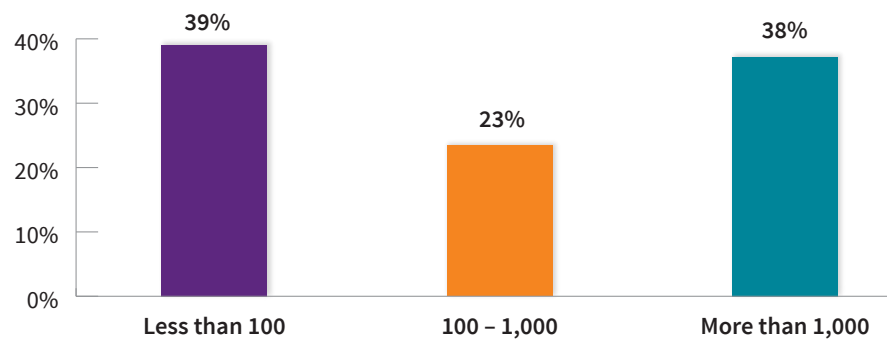
Company size

Q.S3.7: Company size (from sample). Based to those giving a scale response: 771

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

About LexisNexis® Risk Solutions

At LexisNexis Risk Solutions, we believe in the power of data and advanced analytics for better risk management. With over 40 years of expertise, we are the trusted data analytics provider for organizations seeking actionable insights to manage risks and improve results while upholding the highest standards for security and privacy. Headquartered in metro Atlanta USA, LexisNexis Risk Solutions serves customers in more than 100 countries and is part of RELX Group, a global provider of information and analytics for professional and business customers across industries. For more information, please visit www.lexisnexis.com/risk.