

The Many Layers of Cross-Industry Fraud

(UNCOVERING THE HIDDEN CONNECTIONS)

An annual national online survey of 800 fraud mitigation professionals in five industry sectors and government proves there are substantial levels of fraud that touches multiple industries.

Below we highlight key trends in identity fraud and fraud mitigation from the detailed industry report: www.lexisnexis.com/fraudstudy



Insurance



Financial Services



Retail



Government



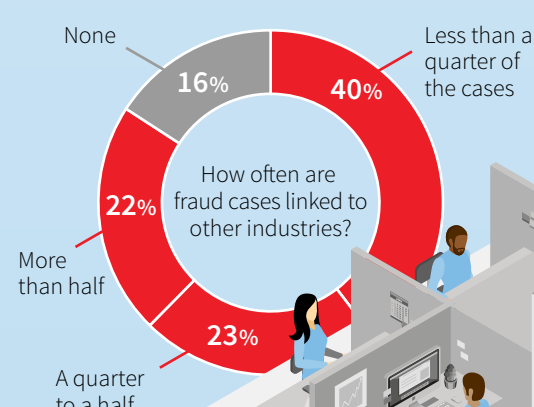
Health Care



Communications

Cross-industry fraud is prevalent

(84% of cases), and 78% of them have a moderate to high financial impact.



The Communications industry reports more of its transactions/services have moved online over the past three years and its top concern is hacking.

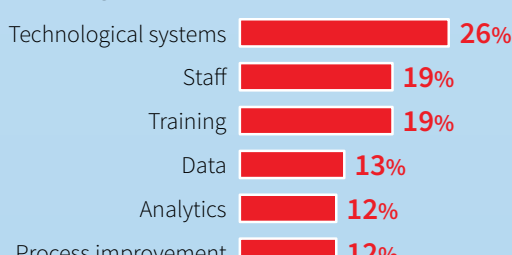
80%

see value in access to outside-industry data

Known fraud data is highly valuable.

Survey respondents see benefits in having known fraud data from other organizations (both inside and outside their industry) for investigations.

Spending priorities to mitigate fraud:



There is a substantial interest in contributory databases.

86% would consider contributing their investigation outcomes into a contributory database in return for data from others.

Insurance respondents most often report that cross-industry fraud cases have a larger impact than those from within their own industry, and outside industry data is considered to be highly valuable to help with fraud investigations.

87%

see value in access to inside-industry data

Smarter data is the new norm.

Automated business rules systems are no longer organizations' top analytics-based solution for fraud mitigation.



Ad hoc database searches and social network graphing round out the top 5.

Health Care respondents cite claims fraud as their highest concern, and they prioritize training as their largest investment.

Highlight: Identity Fraud

Overall, the top fraud concern among all respondents is identity theft/stolen IDs.

60%

have recently moved more of their transactions online, prompting greater concerns about identity fraud with online (vs. offline) purchases.

Top steps to combat identity fraud:

1. Added more identity verification processes that customers must complete
2. Conducted audits of system security
3. Increased use of data analytics for earlier detection of fraud

Business identity fraud:

35%

Among organizations with business accounts, over a third have seen business identity fraud.

Main steps to combat business identity fraud:

1. Increased login/password requirements
2. Business identity authentication requirements for account set-ups

These additional precautions are consistent with the finding that organizations spend more on 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.

Financial industry respondents are more concerned about online transactions than offline, and nearly two-thirds have taken additional steps to protect customers from identity fraud in the past year.

Fraud is prevalent across all industries and mitigation efforts are key to eliminating financial repercussions. By leveraging advanced analytics from contributory databases for known fraud, mitigation professionals can be better prepared to decode the layers of deception, reveal the hidden connections and protect your organization from fraud.

For more information about the LexisNexis 2017 Fraud Mitigation Study, visit www.lexisnexis.com/fraudstudy or call 844.AX.FRAUD (844.293.7283).