White Paper

Enabling Agile and Comprehensive Fraud Defense Through Shared Data

Using cross-industry and cross-sector contributory databases to mitigate fraud.

October 2015

LexisNexis® RISK SOLUTIONS

LexisNexis® Fraud Defense Network

The world is becoming more globalized and interconnected, putting sensitive information at the fingertips of criminals seeking ways to defraud data-dependent systems. While fraudsters are increasingly able to take advantage of this information-rich environment, fraud mitigation professionals often lack the information they need to fight back. As a result, fraud fighters are looking beyond traditionally limited data analytics options for better ways to detect and prevent fraud. Advanced solutions that appropriately leverage data across industries and sectors could be useful. However, despite the fact that the desire for more cross-industry solutions is clear and early efforts in this direction have shown promise, several collaboration challenges remain.

Impact of Fraud

Fraud is prolific, costly and a significant challenge. The estimated cost of fraud varies from about 1 percent to 5 percent of revenue for a typical organization.[1,2] The costs go beyond profit reductions to include increased prices, greater security challenges and damaged reputations. Nearly every sector—from banking to health care to insurance to government—is grappling with the fraud problem in some way, to the collective tune of hundreds of billions of dollars annually in the U.S. alone, and untold trillions globally.

Cross-Industry Fraud: Limited Insights into a Prevalent Problem

Historically, efforts undertaken by organizations to deal with the growing fraud problem, no matter how aggressive in nature, have generally been relegated to business-, agency- or industry-specific practices.

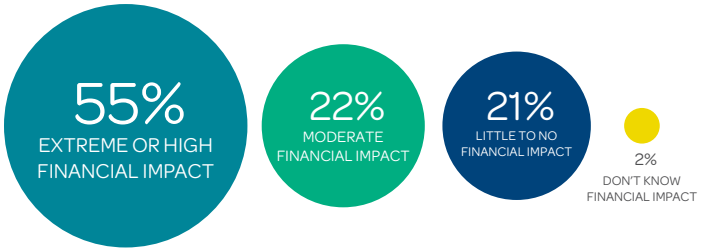
This inward-looking approach is limiting because it does not recognize or address the cross-industry nature of fraud. In fact, the most egregious fraud activity is perpetrated by sophisticated, organized fraud rings or individuals that essentially make their living by engaging in fraud. These professional thieves don't have a particular bias for a given industry or sector. *The New York Times* has reported[3] that the hackers responsible for the Office of Personnel Management (OPM) data breach in 2015, the largest breach of federal employee data in recent years[4], were also responsible for the attacks on health insurance providers Anthem and Premera, two of the largest private sector breaches in recent memory.[5]

Massively coordinated and targeted cyber attacks like the OPM example represent the worst-case scenario, but everyday fraudsters exhibit the same types of cross-over behaviors. For example, someone cheating on or falsifying tax returns may also be falsifying mortgages, automobile insurance claims, health care claims or human services benefit claims. A family in Brooklyn, New York was charged with falsifying income to obtain mortgages and welfare benefits, with charges spanning mortgage fraud, income tax fraud, identity fraud and benefits fraud.[6] Their actions allegedly caused a total of $20 million in fraudulent mortgages and $700,000 in welfare benefits. In another example, a Virginia construction executive fabricated loan applications and used straw buyers to inflate the value of several properties. Her fraudulent actions caused a total of $11 million in losses across the mortgage, banking and income tax sectors.[7]

These examples illustrate how malicious actors follow the easy money and exploit the system for personal gain. Anecdotal evidence of fraudsters' cross-over behavior abounds in the media, but a systematic study of cross-industry fraud was lacking. LexisNexis® Risk Solutions validated—and tested—the concept of cross-industry fraud in a small, internal study comparing data from one industry to others. The analysis showed that if an individual had indicators of suspicious activity in another industry, there was a 2.5 times higher likelihood that person would show up in the suspicious population for the target industry when compared to individuals without such "cross-industry" indicators.

Additional studies seeking to determine the prevalence of cross-industry fraud across the insurance, credit, financial and wider private industry markets have demonstrated how a collaborative approach between industry members can shine a light on previously hidden fraud patterns. In a recent LexisNexis Risk Solutions survey of fraud mitigation professionals, 84 percent of respondents from insurance, health care, government, financial services, communications and retail indicated that they are seeing at least some cross-industry evidence in fraud cases they investigate, and more than three quarters indicated that the impact of fraud that was linked to other industries had a moderate to extremely high financial impact on their organization.[8]

Financial Impact of Fraud Cases Connected to Other Industries



The 2015 LexisNexis® Fraud Mitigation Study asked 400 professionals from insurance, health care, government, retail, communications and financial services about their experiences with fraud cases that touch multiple industries. More than 75 percent indicated that these cases have a high or moderate financial impact on their organization.

Sharing Data for More Effective Fraud Prevention

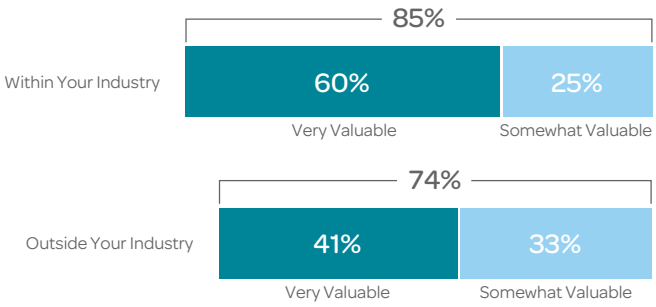
Fraud mitigation professionals have long focused on and invested in anti-fraud measures such as Special Investigation Units, and have implemented business rules systems designed to detect fraud. More recent technological advancements in big data, predictive analytics and social network graphing are providing new and stronger tools in the fraud fight. As a result, business leaders are already seeing higher success rates in identifying fraudulent transactions and improved understanding of fraudulent behaviors.

Despite their benefits, traditional data analytics tools are limited in that they have focused primarily on data sets that are too narrow. This means, for example, that a professional processing a mortgage application may not be aware that the applicant has previously falsified income to obtain a consumer credit card, or that a State Department of Revenue employee processing tax refunds may not realize that the identity of the tax filer is a stolen one.

Imagine if organizations could collectively pool their information about suspicious transactions and share key data points related to their investigations.

There is, in fact, a demand among fraud mitigation professionals to expand their field of vision. In the LexisNexis Risk Solutions Fraud Mitigation study cited earlier, 85 percent of respondents saw value in having access to data about fraud cases from within their industry, and 74 percent saw value in data from other industries.

Perceived Value of Data from Outside Fraud Cases



Respondents to the LexisNexis® 2015 Fraud Mitigation Study indicated that they see value in having access to data and information about fraud cases not only from organizations within their own industry, but also from organizations outside their industry.

A coordinated approach to exchanging information is complex and contains some inherent challenges, but can be accomplished through a cross-industry contributory database, where member organizations contribute potentially fraudulent and suspicious events, allowing members to have access to reported events from other participating organizations. More than just a data exchange, a comprehensive fraud network can also foster communication across a large breadth of organizations to better address this shared problem.

In addition to giving contributors the advantage of a more comprehensive view of a suspect or entity, such an initiative helps organizations detect and intercept fraud before it happens, to safeguard from losses due to fraud. This is significant because traditional "pay-and-chase" models that prioritize recovery over prevention have been exposed as overly costly and less effective than advanced "prevention-based" models that attempt to stop the fraud before it occurs. A contributory database also expedites data access. As organizations gain a clearer view of the fraud landscape ahead of them, they can do more to make informed decisions that will help them navigate that hazardous terrain. Finally, access to information about outside cases helps contributors to respond quickly and accurately with the insights needed at the individual, business or transaction level.

There are several examples of how industry and government have successfully implemented small-scale versions of the contributory data concept:

Government – The National Accuracy Clearinghouse (NAC), is a consortium of five states led by Mississippi and supported by a grant through the United States Department of Agriculture Food and Nutrition Service (FNS) to address the growing challenge of public assistance fraud. The information shared allows participating states to identify dual or multi-state benefits participation and make any necessary fraud-mitigating determinations at the point of application.

Health Care – The National Health Care Anti-Fraud Association (NHCAA) sponsors the Special Investigation Resource and Intelligence System (SIRIS), where members share information regarding fraud cases they have encountered for the purpose of helping to mitigate fraud elsewhere.

Mortgage – Major mortgage lenders, agencies and insurers have for decades been submitting information describing incidents of subscriber verified fraud and material misrepresentation involving industry professionals to an industry-contributed database known as the Mortgage Industry Data Exchange (MIDEX®). Contributing subscribers use information services derived from the MIDEX database as a risk management tool to protect against mortgage fraud perpetrated by industry professionals.

These active examples of collaboratory efforts show that pooling data is possible and beneficial.

Expanding the Concept: Cross-Industry Data Exchange for Fraud Mitigation

Given the propensity of those committing fraud to extend their crimes to multiple industries, it is not difficult to imagine the benefits derived from a broader cross-industry database for fraud mitigation. Internal research conducted by LexisNexis Risk Solutions on a few cross-industry data sets have validated the advantages of a cross-industry database. In a recent Federal Bureau of Investigation (FBI) case in Minnesota, 20 members of an organized crime family were indicted for trafficking stolen and fraudulently obtained smartphones and tablets. It was alleged that these devices were obtained using identity theft and contract fraud schemes and then sold and transported across state lines. Using data from several market areas, LexisNexis Risk Solutions was able to retrospectively identify and flag eight members of the family, which has been described as one of the largest criminal enterprises in Minneapolis-St. Paul. If this cross-industry data had been available to the retail establishments at the time the fraud was occurring, it is likely the fraud may not have continued as long as it did.

In another example, LexisNexis Risk Solutions analyzed data from Property and Casualty insurance carriers and health care organizations and uncovered a medical provider with licenses in multiple states that was facing disciplinary measures in Florida and Illinois. The provider also appeared in multiple Property and Casualty carriers' auto accident injury data with "high alert" status. Providing visibility into the activities of providers like this across the Insurance industry and the health care industry offers the potential to intercept bad behavior earlier.

These examples illustrate that the broader spectrum of data provided through a cross-industry database is the essential missing piece for revealing patterns that would not be evident in one industry or one organization's data alone. By gaining access to a broader scope of information as shared by other contributory system member organizations, both within an industry and across several industries, organizations can create much stronger cases against these entities.

Challenges of Collaboration

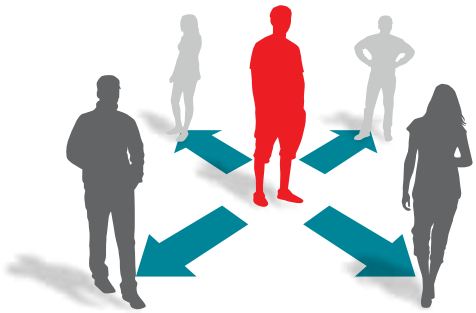
Though the benefits of sharing data seem evident, execution is easier said than done, as a number of barriers to implementation block the path forward. Much must be done to transform the cross-industry information from being just another massive collection of big data into a collection of actionable intelligence.

Linking

The first challenge is accurate identification of common events and entities across markets. Individuals may use different identities and certain businesses may operate under multiple business names. Unless the connections between those different identities are realized, the full extent of the fraudulent activity can't be truly uncovered. It requires a comprehensive and sophisticated linking technology to adequately resolve these apparent differences. In one case LexisNexis Risk Solutions examined, a major property and casualty insurer was in the process of investigating a potentially fraudulent insurance claim, completely unaware that the same person had filed another claim with the same insurer at the same time using a different name. The data associated with the two claims alone wasn't sufficient to indicate this commonality, but through the use of advanced linking, based upon large amounts of additional data, this relationship was discovered.

The second aspect of linking as it relates to cross-industry fraud is the ability to detect relationships *between* entities and activities.

Using Linking to Detect Hidden Relationships



Starting with one potentially suspect auto insurance claim, LexisNexis Risk Solutions was able to link together the relationships between individuals, medical providers and claims to eventually uncover 14 involved individuals on 20 related claims representing almost a quarter of a million dollars in potential losses.

Applying linking to the collaborative arsenal of big data makes it possible to accurately identify individuals, businesses and their relationships, and provide additional insights to fraud investigators. Advanced technology and expanded data can efficiently reveal complex interactions and links between entities, resulting in superior identification of fraud rings and other associations between individuals, businesses, addresses, or transactions that may at first appear innocuous.

False Positives

To balance the pervasive problem of fraud with a limited amount of resource, it becomes very important for fraud teams to focus on the highest risk cases as part of their investigation. It also makes sense to focus more attention on those entities that are systematically defrauding companies than on those who may be opportunistically taking advantage of the system as a one-time event.

While it is not difficult to create long lists of potentially suspicious transactions using current data analytics tools, there will always be a portion of transactions identified as potentially fraudulent that prove to not be fraudulent at all—in other words "false positives."

These false positives cause two problems. First, nobody wants to falsely accuse an applicant, policyholder or customer of fraud. More importantly, every transaction identified by these tools must be investigated and validated, and that takes time and resources. Excessive false positives waste resources, detract from the organizational workflow and potentially damage customer relationships. In certain businesses, like retail, processing orders quickly becomes a significant competitive differentiator and anything that slows down transactions becomes a serious hindrance to profitability. Therefore, it is critically important to bring as much information as possible to bear on each given transaction to minimize the potential for false positives, and create an appropriate balance between the end user experience and proper risk management measures.

Fraud mitigation is not about identifying every incident of fraud—that is not possible, nor realistic. What it is really about is optimizing the investigator's workflow, in other words, maximizing resources to address the cases that matter the most. Doing so requires looking as comprehensively as possible at all relevant data. What a shared data repository can do is enhance an investigator's access to information, to provide a different perspective, allowing the organization to zero in on the cases that truly warrant attention and expedite the ones that do not.

Context and Appropriate Use

Not all information in a contributory database is appropriate in every use case, and indeed, may not be permissible for use in certain cases due to legal or contractual restrictions. This reality means that the original information needs to be classified in various ways so that when it comes time to use it in a given situation it is possible to manage context and appropriate use.

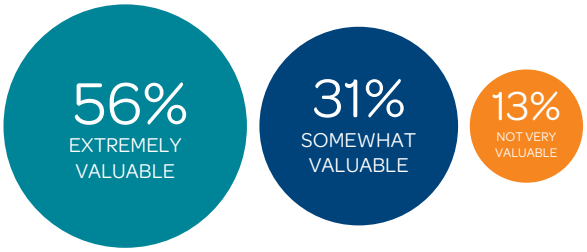
The Importance of Context and Appropriate Use

When it comes to sharing information about fraud investigations, data should be accessed only in ways that provide and enforce usage restrictions so that:

- only contextually appropriate data is presented
- legal restrictions are enforced
- interests of the contributing parties are protected

When it comes time to apply the data in a specific situation, several fundamental questions need to be addressed: "What type of potential fraud does this event represent?", "What about this event provides useful perspective?", "Is this an acceptable use of this particular data?" That's why having a universally consistent way to talk about—or classify—fraud is important. Eighty-seven percent of the LexisNexis Fraud Mitigation study respondents indicated that having a standard way of describing fraud across industries was valuable, with 56 percent indicating that this would be extremely valuable.[10]

Perceived Value of a Universal and Consistent Way to Describe Fraud



The LexisNexis® Fraud Mitigation Study asked respondents about the value they would place on establishing common, general ways of describing fraud that are universal across industries. Eighty-seven percent of respondents saw value, with more than half viewing a universal fraud nomenclature as "Extremely Valuable".

For example, one important dimension of fraud has to do with the nature of the activity. An obvious example is the difference between identity theft and other types of fraud. In the case of identity theft, often the data that is reported is that of the stolen identity; in other words the information is about the victim rather than the perpetrator. If a bank is evaluating an application for credit, the fact that the identity being used was compromised certainly matters and will require a different level of due diligence, but the bank needs to treat the applicant with respect, and not assume he or she is the fraudster. The course of action must be appropriate to the context of the information, and so requires proper classification and management of the data. Similarly, not all types of fraud are the same in severity. Fraud perpetrated by organized fraud rings is generally considered to be more egregious than "opportunistic" fraud, where someone claims damage in an auto accident that wasn't caused by the accident itself.

In some cases, the presence of fraudulent activity will be documented by some type of official body resulting in a criminal conviction or a sanction. This is the most definitive classification of fraud. In other instances, a potentially fraudulent activity may have been investigated and confirmed but no legal or criminal action was pursued because the economics didn't warrant pursuit. These two different classifications of the certainty of potential fraudulent activity need to be handled very differently.

Finally, privacy, security and permissible use also remain rather large hurdles to proper implementation. Not only is it critical to properly capture the context of data and classify it to be able to effectively reuse it across industry boundaries, but it is absolutely essential to properly protect the data. Because of the seriousness of the risk from fraud to the integrity of financial transactions, fraud investigations benefit from many special exemptions in various laws governing privacy and security. However, this data still remains highly sensitive, governed by numerous federal, state and local laws as well as contractual and other obligations. These laws and obligations must be carefully managed across all the data sets provided and across all the potential use applications, and it goes without saying that the physical security of the data is of paramount importance.

Conclusion

In most cases, there are telltale signs that reveal potentially fraudulent behavior and opportunities to enact proactive measures to help mitigate risk. Implementing a cross-industry culture of collaboration and information sharing promises many significant benefits to preventing fraud across all organizations.

To truly leverage the maximum value that lies within contributory data, there must be the proper framework for information usage and sharing. As these obstacles are overcome, industries will be in a position where they can detect and intercept fraud as it is attempted, protecting their bottom lines from the historical menace of fraud, waste and abuse. By leveraging an informed cross-industry view, executives will be able to optimize their processes with access to a collaborative framework that provides them not only comprehensive information, but also the tools to put that information into a usable context.

By leveraging the whole spectrum of information currently in the hands of industry partners and government agencies, fraud investigators could benefit from more effective fraud detection and prevention.

For more information:

Call 844.293.7283 (844.AX.FRAUD) or visit lexisnexis.com/FDN

About LexisNexis Risk Solutions

LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government assess, predict and manage risk. Combining cutting-edge technology, unique data and advanced analytics, LexisNexis Risk Solutions provides products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of RELX Group plc, a world-leading provider of information solutions for professional customers across industries.

LexisNexis® RISK SOLUTIONS | LexisNexis® Fraud Defense Network

[1] Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study, Association of Certified Fraud Examiners, p. 8.

[2] 2015 LexisNexis® True Cost of Fraud Study, September, 2015.

[3] David E. Sanger, Julie Hirschfeld Davis and Nicole Perlroth, "U.S. Was Warned of System Open to Cyberattacks," The New York Times, June 5, 2015.

[4] Ellen Nakashima, "Chinese Breach Data of 4 Million Federal Workers," The Washington Post, June 4, 2015.

[5] Jeremy Kirk, "Premera, Anthem Data Breaches Linked by Similar Hacking Tactics," PCWorld (online), March 17, 2015.

[6] "Fourteen Defendants Charged in White Plains Federal Court with Massive Mortgage Fraud Conspiracy," www.fbi.gov, Nov. 13, 2014.

[7] Jeff Sturgeon, "Grand Jury Indicts Roanoke Woman in Smith Mountain Lake Land Scheme," The Lynchburg News & Advance, June 19, 2014.

[8] LexisNexis® 2015 Fraud Mitigation Study: Summary of Key Findings, published Aug. 2015, accessed via http://www.slideshare.net/LexisNexisRisk/358890-In-fdnslidesharerd87/1

[9] Ibid.

[10] Ibid.