White Paper

A Unique Perspective into the World of Identity Fraud

Explore the value of LexisNexis® FraudPoint® solutions in fraud detection.

LexisNexis®

Risk Solutions
Identity Management

Executive Summary

There are many challenges in detecting identity fraud. These challenges are magnified by the lack of an industry-wide repository of 'identity information'. While credit risk information is traceable to a single consumer, identity fraud is often untraceable to the fraud perpetrator, who can simultaneously affect multiple consumers and accounts. In addition, while a great deal of identity fraud is the result of a stolen identity, there are growing trends in many fraud schemes such as synthetic identities, manipulated identities and friendly fraud.

An identity repository to trace and monitor how identities are created and modified over time would enable better fraud mitigation strategies. Boasting over 35 years of experience as the largest compiler of consumer identity information, LexisNexis® has built one of the largest and most comprehensive commercial identity fraud prevention repositories in the nation. This identity repository has proven to be highly effective in combating identity fraud.

Identity fraud remains an ongoing problem

Fraudulent credit behavior is a significant problem for the financial services industry. According to the Federal Trade Commission (FTC), 19% of complaints to its Consumer Sentinel Network in 2010 were related to identity theft. In total, the number of identity theft complaints has tripled between 2001 and 2010. Importantly, these statistics are based on victim reported frauds to the FTC, and are likely an underestimate of actual identity theft rates and losses. In February 2012, Javelin Strategy released its annual Identity Fraud Report—often used as a benchmark for identity fraud trends—and reported fraudulently opened new accounts drove losses of $5 billion across 1.95 million victims in the United States in 2011. Furthermore, consumers reported that they are increasingly spending more of their money and time to remediate the effects of application stage identity fraud, with average consumer out of pocket costs of $1,205 per event, the highest reported over the past 6 years.

3x

The rate at which identity theft complaints have risen between 2001 and 2010.

Among the challenges in detecting identity fraud is the way identity information is organized for fraud detection. While credit risk is traceable to a single consumer with a single payment history across all accounts; fraudulent identity manipulation is often untraceable to the fraud perpetrator, who can simultaneously affect multiple consumers and accounts and adapt to defeat preventive measures. Additionally, the definitions of credit risk and fraud vary by institution, resulting in inconsistent labeling of fraud across lenders. An authoritative identity repository would resolve this challenge, resulting in more effective detection within the vastly larger universe of normal identity variation.

Identity fraud has traditionally been defined as the unauthorized use of another's personally identifiable information to achieve financial gain. While a great deal of credit fraud is the result of stolen identity, there has been a rise in the manufacture of synthetic identities or the creation of alternative versions of existing identities that are "close enough" to pass casual scrutiny. In order to capture these growing trends of falsifying identities, LexisNexis has broadened the definition of identity fraud to include any material misrepresentation of an identity fact in the course of opening or gaining access to a financial account. This definition includes stealing the identity of an unsuspecting victim, inventing a synthetic identity, or managing an altered version of an existing identity.

LexisNexis compiles identity facts

LexisNexis® Risk Solutions has a unique vantage point to observe the identity activity of U.S. consumers. Boasting over 35 years of experience as the largest compiler of court documents, public record filings, state licenses and registrations, property deeds, phone and address change information, bankruptcy proceedings and other proprietary and licensed data sources, LexisNexis has built the largest and most comprehensive identity fraud prevention database in the nation. Comprised of more than 34 billion records from more than 10,000 sources and growing daily by millions of records - the identity repository enables all of the LexisNexis identity solutions used by thousands of financial institutions. In total, the LexisNexis identity repository had 290 million active identities on file on January 1, 2012, of which just over 7 million identities were newly reported in 2011.

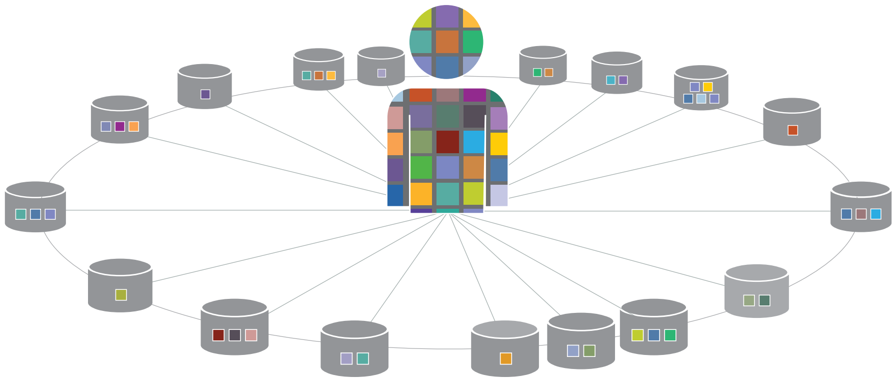
This identity repository is the core of LexisNexis® FraudPoint® Score and LexisNexis® FraudPoint® Attributes, a new patent-pending identity fraud solution that is unique in its use of a multi-dimensional identity bureau to detect suspicious or fraudulent events. By monitoring identity information from multiple data sources, the FraudPoint Solution achieves a robust view of identities by examining four categories of identity information:

- **Category #1: Tri-Credit Bureau Identity Activity**
  Identity information from three national credit bureaus is monitored for all the identity events that financial institutions report during their normal updates to the credit reporting agency. FraudPoint can see every identity reported to the credit bureaus, including the full name, Social Security Number (SSN), and current address. Tracking credit header identity information captures both new identities and changes to existing identities such as the reporting of a new address or the discontinuation of reporting. Identities on file at credit bureaus are necessary but not sufficient because fraudster invented identities are reported alongside identities of legitimate credit users.

- **Category #2: LexisNexis Customer Network**
  FraudPoint has visibility to millions of inquiries from financial institutions confirming identities of consumers attempting to open new financial accounts. These records give FraudPoint insight into the recency and velocity of identity usage, and the frequency of identity misuse. Not all of the identities seen in our identity verification inquiries represent real people, and insight into identity misuse (e.g. multiple recent queries about unknown individuals, all using the same home address and phone number) can be very useful in detecting fraud ring activity.

- **Category #3: Online, Utility, Phone and Other Identity Activity**
  FraudPoint monitors identity activity reported by landline phone carriers, utility reporting services, and mobile phone directories to track confirmed address changes in near real-time. This dimension provides a very timely source of address changes and current residential status; as well as providing identity coverage on millions of U.S. consumers who are unknown at the credit bureaus.

- **Category #4: Local, State and Federal Government Records**
  FraudPoint reviews government reported public record data sourced from county courthouses and all fifty state governments such as real estate property deed transfers, county property tax records, court judgments, felony and criminal convictions, tax liens, evictions, occupational licenses, drivers licenses, vehicle and watercraft registrations, voter registrations, bankruptcy filings and related records. Tens of millions of identities that have no credit bureau presence or utility records are found in these government and court sources. These sources are difficult to manipulate or falsify. FraudPoint also searches student directory sources compiled from college and university sources to more accurately check identities of young adults, many of whom have little or no presence in other data sources.



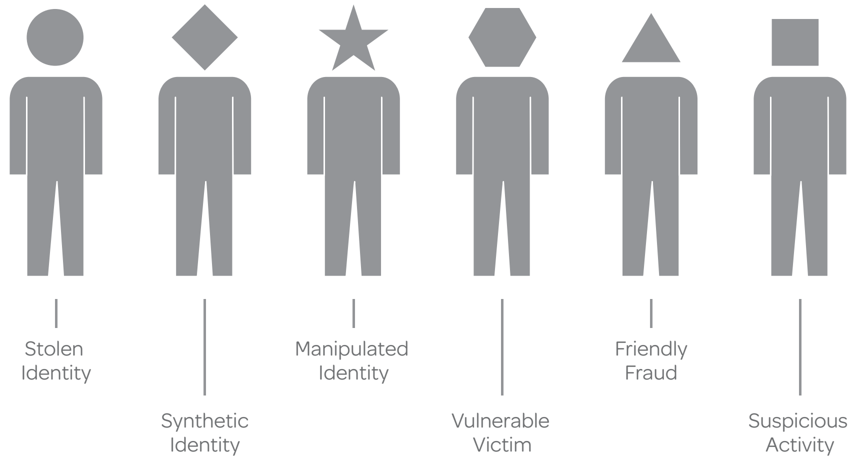
FraudPoint takes the information from all these categories and examines the full identity footprint across all sources, looking for points of consistency and/or anomaly that indicate likely fraud. FraudPoint considers: the identity's originating source (such as driver's license, voter registration, credit bureau header update, etc.), its time in the identity repository, the number of sources confirming the identity, the variation in identity elements across sources, the frequency with which the identity was used for applications, the number of associated identities (especially suspicious ones), etc. By comparing millions of normal identities with rarer suspicious identities, FraudPoint is able to profile applications with high risk identities into their likely fraud type.

FraudPoint considers:

- The identity's originating source (such as driver's license, voter registration, credit bureau header update, etc.)
- Its time in the identity repository
- The number of sources confirming the identity
- The variation in identity elements across sources
- The frequency with which the identity was used for applications
- The number of associated identities (especially suspicious ones), etc.
- And more

For example, an identity that is seen only in credit bureau header data, but not on any other data source, is at higher risk of being a synthetic identity, especially if the address has a high velocity of credit seeking, and multiple suspicious identities are using the same SSN. FraudPoint differentiates six types of risky identities: Stolen, Synthetic, Manipulated, Vulnerable Victim, Friendly Fraud, and Suspicious Activity.

FraudPoint Differentiates Six Types of Risky Identities



Breadth of the problem

LexisNexis has recently conducted an investigation into the magnitude of suspicious identity behavior and subsequent fraud rates. In examining the behavior of different samples, key fraudulent claims come to light. From this investigation, LexisNexis was able to identify specific fraud trends and other identity anomalies.

Method

The LexisNexis research team examined the identity repository information from two different perspectives to better understand fraud trends. First, we studied the identities used to apply for new financial accounts in December, 2011 in order to understand the patterns of suspicious identity elements detected by FraudPoint solutions. Second, we studied the identities used to open credit accounts in early 2011 in order to understand subsequent fraud-loss rates.

Results

Study 1

The majority of new account applications screened against our identity repository have no apparent identity issues. Over ninety percent of applications are fully verified with no evidence of stolen identity, created identity or identity manipulation. Five percent of applications are from new identities that have not previously been seen by a major credit bureau, and most of these appear to be legitimate consumers opening their first account.

There are also a significant number of very suspicious applications mixed in with all the normal account opening transactions. More than one percent (1.5%) of applications are from identities associated with five or more different Social Security Numbers (SSN) in the identity repository. Almost one percent (0.9%) of applicants used an SSN that is linked to a different identity at a different address.

Some applications looked suspicious in their misuse of SSN or address information other than their own. Fully 3.0% of through-the-door applications showed significant evidence of stolen identity.

- 24 - 5555
- 23 - 5555
- 23 - 5545
- 23 - 5546
- 99 - 1234

1.5% of applications we examined are from identities associated with five or more SSNs.

The analysis then focused on the number of synthetic or created identities presented at account opening. Of those identities appearing for the first time, more than two percent used an SSN that was reported as deceased or that was issued to someone else before the applicant's claimed date-of-birth. Many of these identities had been used on multiple applications in the recent past, and often shared an address with multiple suspicious identities and applications. About 1% of all applications showed significant evidence of being a synthetic identity.

Study 2

With the magnitude of attempted fraud quantified in the 2% to 5% range across multiple financial institutions and account types, we focused on fraud incidence rates in a particularly industry: revolving credit card issuers. Analysis of over 2,500,000 bankcard applications profiled the identity characteristics of known fraud cancels, known fraud losses, and first-pay defaults. First payment defaults were included if they became untraceable after opening an account, using the card, and making no payments. These were included because a review of their characteristics showed that they looked more like fraudulent identities than like normal credit defaults. This combined definition of fraud yielded a 1.3% fraud rate for the entire sample.

Applications where the SSN was reported to belong to someone other than the applicant had a 24% fraud rate. If the SSN was reported deceased or was issued prior to the applicant's date-of-birth, the fraud rate was over 21%. Where there was significant evidence of stolen identity, the fraud loss rate was 43.2% on over 30,000 applications. Where there was significant evidence of synthetic identity, the fraud loss rate was 24.2% on over 12,000 applications.

Overall, FraudPoint Score effectively rank ordered fraudulent applications (see the table below). In the lowest tail of FraudPoint Score, corresponding to a 350 cutoff, fraud rates are as high as 58.2% and almost one-third (31.5%) of all fraudulent applications are identified while sacrificing less than one-half of one-percent of non-fraudulent applications (0.3%). Using a more typical cutoff of 550, 71.1% of all fraudulent applications are identified while only forgoing 3.5% of non-fraudulent applications. In short, FraudPoint Score effectively identified future frauds with a very low false-positive rate.

43.2%

Where there was significant evidence of stolen identity, the fraud loss rate was 43.2% on over 30,000 applications.

Effectiveness of FraudPoint Score in Identifying Future Frauds

FRAUDPOINT SCORE BAND	CORRESPONDING SCORE CUTOFF	FRAUD RATE PER SCORE BAND	CUMULATIVE % OF FRAUDS IDENTIFIED BELOW CUTOFF	CUMULATIVE % OF NON-FRAUDS IDENTIFIED BELOW CUTOFF
300-349	350	58.20%	31.50%	0.30%
350-399	400	33.40%	45.20%	0.60%
400-449	450	19.60%	56.70%	1.20%
450-499	500	9.80%	64.80%	2.20%
500-549	550	5.60%	71.10%	3.50%
550-599	600	2.80%	76.60%	6.00%
600-649	650	1.40%	82.30%	11.00%
650-699	700	0.60%	88.60%	23.70%
700-749	750	0.30%	95.70%	56.90%
750-999	999	0.10%	100.00%	100.00%
Population Average		1.30%		

- In the lowest tail corresponding to 300-350 scoreband cutoff, fraud rates are as high as 58% and almost one-third of all fraudulent applications are identified—while sacrificing less than one-half of one percent on non-fraudulent applications.

- Using a more typical cutoff of 550, 71% of all fraudulent applications are identified while only forgoing 3.5% of non-fraudulent applications.

Cases of interest

In the course of our investigations we found several interesting cases that are worth highlighting to demonstrate how manipulated identities differ from normal identities.

- One SSN was used by 57 unique names, each living at a different address.
- One identity was the subject of 33 consumer application attempts in a one month period. All applications used the same SSN and address; but the names and birthdates used corresponded to two different unrelated applicants.
- A 34 year old identity that declared bankruptcy in 2000 was the subject of 130 attempts to open credit in December 2011. At least 116 different SSNs were submitted across these attempts.
- A 71 year old identity was the subject of 67 attempts to open credit. The fraudster used 54 different SSNs and 2 different birthdates.
- A 44 year old identity was the subject of 42 inquiries. The inquiries were associated with a variety of apartment numbers from the same building, in which the identity doesn't appear to have ever lived.

In short, by observing the interrelationships between identity elements, LexisNexis is able to flag applications that are at high risk of identity fraud. Indeed, each of the above cases was identified by FraudPoint as an application with high probability of being a case of identity theft.

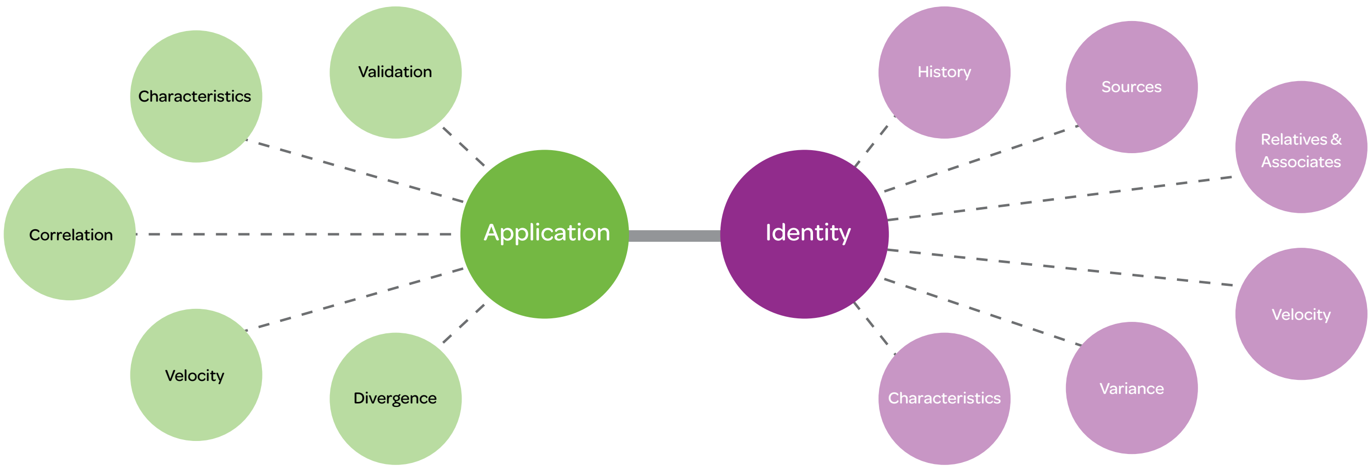
Putting it all together: FraudPoint solutions

FraudPoint provides lenders with the intelligence to better predict and prevent identity fraud. With access to the most comprehensive identity fraud prevention repository, FraudPoint solutions deliver a robust foundation for fraud prevention. These predictive tools help lenders quickly detect fraud threats while minimizing false positives.

FraudPoint solutions allow lenders to:

- Identify fraud incidents before the application is booked
- Reduce fraud losses and/or achieve fraud loss goals
- Minimizes administrative costs associated with inefficient and unnecessary investigation

Benefits of FraudPoint Solutions



FraudPoint solutions provide visibility into the application profile and the applying identity to detect multiple forms of identity fraud.

Detecting the "needle in the haystack"

Unique patent-pending segmentation is the key to successfully detecting rare "needle in a haystack" outcomes like fraud. Rather than applying a single methodology to all applications, FraudPoint focuses on identity combinations to differentiate between different fraud schemes. Separate scoring systems were created to detect synthetic identities, stolen identities, manipulated identities, friendly fraud, vulnerable victims, and suspicious identities.

The FraudPoint solutions also help lenders identify and investigate fraud through its four delivered components. First is a three digit FraudPoint Score to provide a high-level probability of an application being fraudulent. Second is a series of Fraud Risk Indices that provide lenders guidance on the type of fraud scheme being perpetrated. Third are Fraud Warning codes to provide specific guidance on identity problems. Fourth are a set of over 200 model-ready, highly-predictive FraudPoint Attributes that can be used in custom fraud and identity theft models. The FraudPoint Attributes contain information not found in other identity aggregator solutions.

For more information

Call 866.858.7246 or visit lexisnexis.com/risk/financial-services

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 predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide 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 Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

FraudPoint Solutions are not provided by a "consumer reporting" agency as that term is defined in the Fair Credit Reporting Act (15 U.S.C. § 1681, et seq.) ("FCRA") and do not constitute "consumer reports" as that term is defined in the FCRA. Accordingly, FraudPoint Solutions may not be used in whole or in part as a factor in determining eligibility for credit, insurance, employment or another purpose in connection with which a consumer report may be used under the FCRA.

Due to the nature of the origin of public record information, the public records and commercially available data sources used in reports may contain errors. NXR01902-1 0313