id:analytics®

WHITEPAPER

Address Discrepancy Data Study

Change of Address and Address Mismatch

December 2009

Table of Contents

Executive Summary

ID Analytics recently conducted a study to examine the relationship between changes in address and fraud risk. The purpose of the study was to determine whether certain variables related to an address change indicate greater risk of fraud. The study also explored whether those address change variables can be used to help organizations reduce fraud losses and operational expenses associated with investigating and confirming change of address requests.

Requesting a change of address on an account is a common tactic used by fraudsters to gain access to an account's assets. Once the fraudulent address is in the system, the fraudster can then place orders for replacement credit cards, checks, passwords/PINs or new cell phones which will be mailed to the fraudulent address. Account take-over (ATO) and other frauds linked to address changes are costing companies millions of dollars each year.

Similarly, millions of credit reports are purchased each year with address discrepancies — the application address and the credit bureau address do not match. The Fair and Accurate Credit Transactions Act (FACTA) requires that in these situations, lenders, wireless providers and utility companies verify the address discrepancy through a different source of information. The vast majority of these address mismatches are harmless, but the required verification can be costly and cause unnecessary customer friction.

Understanding address risk is also important for eCommerce merchants. For online transactions, high fraud rates often stem from orders where the "ship to" and "bill to" address do not match. By understanding and distinguishing legitimate differences, such as in the case of gift giving versus actual fraud, retailers can capture a greater share of revenue, save millions of dollars in fraud-related losses each year, and reduce customer abandonment.

Distinguishing address changes resulting from legitimate consumer moves from those of fraudsters attempting to take-over a consumer's account or identity is an ongoing identity management challenge. Organizations across a wide array of industries including financial services, utilities, eCommerce and telecommunications struggle to effectively identify fraudulent address changes. And with new Federal regulations placing more stringent responsibilities on creditors to resolve address discrepancies, creditors have more incentives than ever to resolve the risk associated with an account address change.

Americans are constantly on the move. According to the U.S. Census Bureau, 40 million Americans (13 percent of the population) move to a new address each year. As organizations try to keep up with this highly mobile consumer population, they face persistent identity risk challenges.

This paper explores methods of predicting risk associated with a change of address. It evaluates several metrics traditionally used to predict address change risk, including: (1) comparative area income levels, (2) distance of a reported move, and (3) whether certain move patterns are riskier than others. **It concludes that, while each of these variables can help predict address change risk for a small subset of the population, none of these variables alone can provide comprehensive risk coverage.**

As an alternative, ID Analytics set out to assess the predictive power of identity risk scoring for address change events. The company's patented identity risk scoring technology is currently used by leading financial institutions, retailers, government agencies, healthcare providers and telecommunications providers to assess identity fraud risk at account opening. The study of over two million address changes indicated that ID Analytics' technology accurately and comprehensively predicts address risk.

Introduction: Why Address Changes Matter

Americans are constantly on the move. According to the U.S. Census Bureau, 40 million Americans (13 percent of the population) move to a new address each year. As organizations try to keep up with this highly mobile consumer population, they face persistent identity risk challenges. In particular, organizations need to distinguish address changes as a result of legitimate customer moves from fraudsters' efforts at ATO.

Identity fraud associated with address changes has serious economic consequences. According to the Federal Trade Commission's (FTC) most recent national survey of identity fraud, the 2006 Synovate survey, three percent of adult Americans or 6.5 million people, annually suffer misuse of their existing credit cards or other non-credit accounts, such as checking, savings or wireless accounts, leading to billions of dollars in losses. Ten percent of the existing account fraud victims surveyed by the FTC directly attributed their losses to ATOs.

How does a typical ATO scheme work? ATO involves the take-over of an existing legitimate consumer account by a fraudster. In a typical ATO scheme, a fraudster acquires an individual's personal information (e.g. account number, name, Social Security number), and uses this information to contact the account issuer to change the legitimate mailing address, phone number or email address to one controlled by the fraudster. Generally, the fraudster follows up this change with a request for a new bankcard, checks, or PIN to ultimately gain access to the legitimate account holder's assets. For wireless accounts, the fraudster typically orders a new device.

Understanding the risk of address change has broader implications than just ATO. An incorrect address can lead to pulling the wrong consumer's credit bureau file, or require additional manual verification, which can substantially increase an organization's operational costs. Address change risk can also adversely affect the credit risk of a consumer.

Perhaps, the most compelling reason for companies to focus on address changes is compliance. In 2007, under the auspices of FACTA, Federal financial regulators and the FTC published new rules to assess the identity theft threat posed by address changes. These new rules, issued concurrently with FACTA's Red Flags Rules, require users of consumer credit reports to scrutinize address changes for existing customers, as well as new account applications where the application address differs from the information maintained by the three national credit bureaus. There are also special requirements for verification when a change of address request is followed by a request for a replacement credit or debit card.

A 2009 Fraud Management Institute survey found that banks could spend an estimated $300 million per year on change of address confirmation letters alone, just to meet compliance obligations. Many survey respondents reported that they are spending considerably more time on FACTA compliance than originally anticipated.

In addition to new compliance and business challenges, the deep economic recession of 2008 and 2009 has put a new twist on address change risk. For example, the traditional methods for assessing the risk of address change may no longer be effective. Address change "markers" traditionally indicative of fraud are now merely reflective of the economic situation. This includes moving from a high-income ZIP Code to a low-income ZIP Code, or moving from a single-family home to a multi-family dwelling. To cost-effectively comply with new Federal regulations and to protect against ATO, a new analytic approach to accurately evaluating address discrepancies is needed.

The ID Analytics Change of Address Data Study

ID Analytics conducted a change of address data study to gain insight into address fraud risk and to assist creditors in complying with Federal regulations. The study used as its data source the information in the proprietary ID Network®. Built with the specific purpose of preventing identity fraud, the ID Network is the largest cross-industry fraud consortium in the world. It houses 700 billion total aggregated data elements, 2.6 million reported identity frauds, and 1.4 billion consumer transactions. With a constant stream of input from Fortune 100 companies, the ID Network receives an average daily flow of 45 million identity elements. The ID Network contains address information from 2002 through the present.

The study first examined the predictiveness of two attributes, or rules, commonly used to design address change validation rules: (1) comparisons of the relative household income at the old and new ZIP Codes, and, (2) distance moved. ID Analytics also created a new rule that has not historically been used in analyzing the fraud risk of a change of address: specific address-to-address combinations. For this study, ID Analytics used the vast data in the ID Network to determine if there are specific address-to-address combinations that are more risky than others. For instance, is a move from Town A to Town B a relatively riskier move than from Town X to Town Y in the U.S.?

The study then analyzed address risk through network-based variables statistically combined into an identity risk score.

1. Changes in Income Class

Traditionally, reported moves associated with changes in income class, especially in the downward direction, based on ZIP Code or other geographic data, are considered indicative of potential fraud. ID Analytics measured the effectiveness of this variable by looking at over 68 million address changes over the period of January 2004 to October 2008 in the ID Network. The study broke down income classes into three categories: (1) high, (2) medium, and (3) low. A high-income address was defined as greater than $52,000. The study further defined a medium-income address as $30,000 to $52,000, and a low-income address as less than $30,000. The study concluded the address change was a fraudulent event if the move was linked to a fraudulent event in the ID Network.

The study found moderately higher fraud rates in reported moves between areas of different income levels. For example, address changes from medium-income to high-income areas had a fraud rate of 0.56 percent. As seen in Figure 1, the vast majority of address changes (93.8 percent) were within the same level of income. These like-income changes of address reflect the lowest fraud level of any combination.

INCOME CLASS CHANGE AND FRAUD RISK

INCOME CLASS	FRAUD RATE MOVES	PERCENT
Medium to High	0.56%	2.53%
High to Medium	0.53%	2.50%
Low to High	0.45%	0.05%
Low to Medium	0.41%	0.51%
High to Low	0.34%	0.06%
Medium to Low	0.29%	0.55%
High to High	0.28%	21.56%
Medium to Medium	0.25%	67.57%
Low to Low	0.16%	4.68%

Figure 1: Any reported move between income class, either up or down, generally indicates a higher degree of fraud risk. However, the vast majority of moves are within the same income level.

Contrary to conventional wisdom, downward income address moves from high-income to low- or medium-income yielded only a moderate increase in fraud rates. Surprisingly, upward income level moves of low-income to high- or medium-income areas resulted in higher fraud rates.

The highest fraud rates were the high- to medium-income, and medium- to high-income level move combinations at 0.53 percent and 0.56 percent respectively. The percentage of reported moves in this category was also higher than the combinations that included lower income moves.

Surprisingly, the data suggests that the highest fraud rates in income level comparisons between old and new addresses originate in the high- or medium-income level combinations, as opposed to the previously theorized high- to low-income level combination.

The study also revealed that looking at income indicators in evaluating address changes has limited value because most address changes do not involve a shift in income level. Almost 94 percent of the address changes studied did not involve a change in a move to an area of a differing income level. In economic downturns, this variable might have slightly more prevalence as individuals move from high- to medium-income neighborhoods and from medium- to low-income areas.

2. Distance as a Predictor of Fraud Risk

The data study also examined the impact of distance traveled between old and new addresses. Again, the study looked at over 68 million address changes within the ID Network over a four-and-a-half year period of time.

Compared to income changes, the study found moving distances provide better predictive qualities in assessing fraud risk. For reported moves within cities such as New York, Chicago and Washington, D.C., the shorter the move distance, the lower the fraud rate. As shown in Figure 2, reported moves of greater than 100 miles were almost four times more indicative of fraud than those moves of less than 25 miles (0.93 percent versus 0.23 percent). This variable, like income variation, only applies to a very small portion of the moving population. The vast majority of reported moves — over 95 percent — occur between addresses that are less than 50 miles apart.

DISTANCE AS A PREDICTOR OF FRAUD RATE

MOVE DISTANCE	FRAUD RATE PERCENTAGE	PERCENTAGE OF MOVES
Within 25 Miles	0.23%	84.77%
Within 50 Miles	0.40%	11.10%
Within 100 Miles	0.67%	3.24%
More than 100 Miles	0.93%	0.89%

Figure 2: Most reported moves are shorter than 25 miles. On average, the longer the move, the higher the fraud rate.

Because four times more fraud occurs in reported moves of over 100 miles and the volume of those moves is much smaller, the distance of a move is a far better predictor of identity risk than shifts in income level.

3. Examining Specific Move Patterns

The study then examined whether there are specific reported move patterns that are riskier than others for reported moves between certain Sectional Center Facilities (SCFs), which are represented by the first three digits of a ZIP Code. In the U.S., there are 860,000 SCF to SCF move combinations.

At the time of the study, there were approximately 2,300 SCF move combinations within the ID Network with 10 or more instances of reported moves per combination that were evaluated. SCF move combinations with less than 10 reported move pairs were eliminated because the sample was too small for statistical significance. The average fraud rate for this population was 0.27 percent.

There are over 1.8 billion 5-digit ZIP Code move combinations, which make comparing 5-digit ZIP to ZIP combinations impractical for this analysis. Additionally, we expect that many 5-digit ZIP to ZIP combinations have specific combinations which are too small to be statistically significant.

As with income, the analysis shows that the vast majority of reported moves are within the same three-digit SCF. Similarly, this type of move within an SCF reflects lower fraud rates than moves outside of a given SCF. Reported moves within SCFs are generally less than half as risky as the average move (0.11 percent), compared to the average fraud rate of 0.27 percent.

EFFECT OF SCF REPORTED MOVES ON FRAUD RATE

SCF PAIRS	REPORTED FRAUD	TOTAL MOVES	FRAUD RATE
379,482	48	146	32.88%
378,482	17	111	15.32%
194,112	46	511	9.00%
458,482	21	247	8.50%
111,191	30	434	6.91%
006,100	63	928	6.79%
125,191	14	212	6.60%
110,191	12	202	5.94%
100,191	232	4040	5.74%
800,112	12	216	5.56%
101,191	21	383	5.48%
432,331	13	256	5.08%
103,191	26	528	4.92%
117,191	42	867	4.84%
852,112	25	566	4.42%
100,194	18	412	4.37%
115,191	25	590	4.24%
009,100	74	1776	4.17%
891,482	24	578	4.15%
105,191	16	388	4.12%

Figure 3: The twenty riskiest SCF to SCF move combinations indentified in the study.

The results also showed that the 100 riskiest SCF move combinations are 17.6 times more risky than the average move. This confirmed that there are specific SCF to SCF combinations that are extremely risky, and some of which appear to be related to specific fraud rings. With some notable exceptions (for example, moves within cities such as New York, Los Angeles, Detroit, San Francisco and Oakland), reported moves within SCFs are generally less than half as risky as the average move.

Just as with income changes and distance variables, reported moves between SCFs do not encompass a broad swath of the moving population. Again, the 100 riskiest move patterns reflect only a minor percentage of the 860,000 SCF to SCF move combinations.

Our analysis of traditionally used address risk variables—distance moved and change in income levels—showed that, while moderately predictive for a small subset of the population, these variables do not cover an adequately broad spectrum of the population to be seen as reliable measures of address risk.

While SCF pairings are more predictive than these conventional variables, they are also limited in scope.

Using Network-Based Identity Scoring to Measure Address Risk

After finding that conventional variables and a newly created address risk comparison had limited predictive value, ID Analytics investigated an alternative approach, looking at the use of identity risk scoring to evaluate change of address risk.

ID Analytics surmised that change of address risk is not a standalone fraud problem, but a subset of the more general threat of identity fraud. Traditional change of address risk models ask the conventional question "Is this address change risky?" Applying network-based identity scoring to change of address risk answers a slightly different but equally relevant question: "Does this specific change in address suggest an increase in the overall risk of this specific identity?"

IDENTITY FRAUD CHARACTERISTICS		
	APPLICATION FRAUD	ACCOUNT TAKEOVER
IDENTITY THEFT TIMING	Account opening	Any time in account life
IDENTITY THEFT EVENT	Application for credit	Non-monetary change Card/PIN issuance
IDENTITY THEFT APPROACH	Criminal asserts identity using victim SSN, Name and DOB Criminal alters Address and Phone Number	Criminal maintains victim SSN, Name and DOB Criminal alters Address and possibly Phone Number

Figure 4: The identity fraud characteristics of account take-over fraud are very similar to those in application fraud; however, they occur at a different time in the account's lifecycle.

ID Analytics identity risk scoring technology has proven highly effective in identifying fraud at the point of account origination for industries such as banks, credit card issuers and wireless service providers. As shown in Figure 4, the identity fraud characteristics in ATO are very similar to those in application fraud, except ATO risk occurs at a different time in the account's life such as during a nonmonetary change like the issuance of a new card or a PIN.

ID Analytics hypothesized that identity risk variables would prove more predictive than traditional variables for several reasons. First, identity scoring looks at multiple variables at once including fraud, verification and velocity attributes such as Social Security number linked to multiple addresses, old or new address validity, and unusual number of recent applications at the old or new address.

While some identity risk variables are standalone, such as "address is invalid," other variables assess suspicious linkage patterns among addresses and other identity elements, such as an unusual number of recent applications using a single address. Single order matching alone will not work. To be truly effective, linkage patterns must expand to at least second order matching. For instance, it is less important to understand what address an applicant or account holder moves to. It is much more important to understand the behavior patterns associated with the address that the individual identity is moving to and what other individuals are moving to that address.

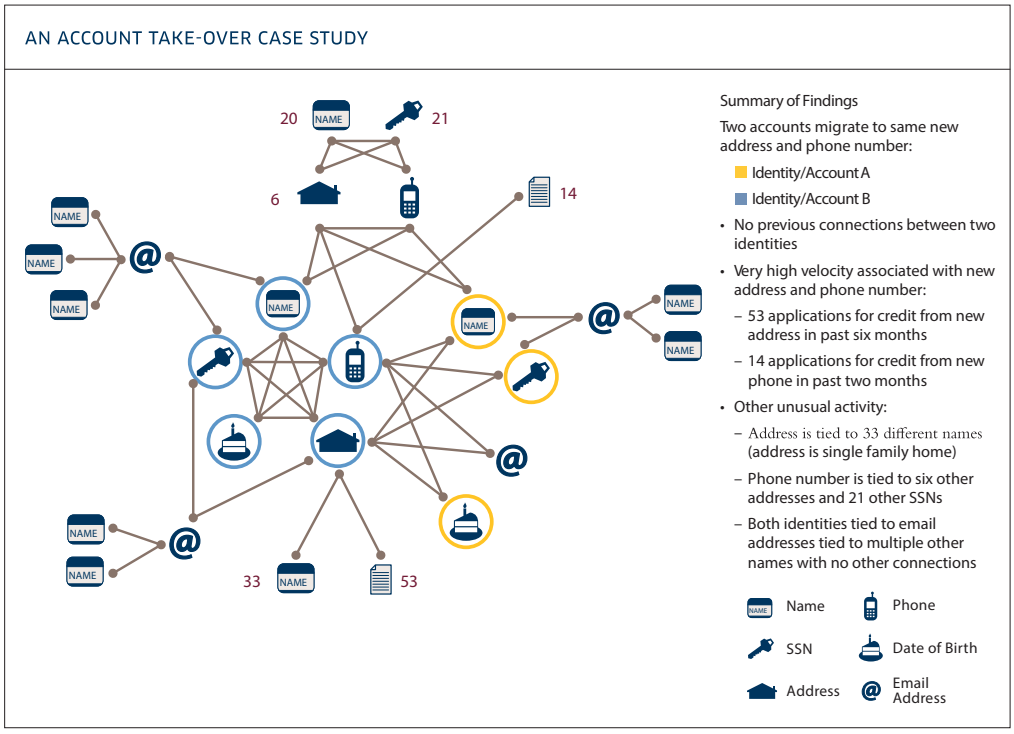

Figure 5: An example of ID Analytics' patented approach to multiple order linkage representing an account take-over case study.

As shown in Figure 5, identity scoring also looks at address risk in the context of a larger calculation of identity risk. An address is just one of hundreds of interrelated identity variables that contribute to a holistic view of identity risk. In addition to address, identity risk scoring also examines the use of other identity variables such as name, phone number, Social Security number, date of birth, and reported fraud information. With this approach, an old or new address is like any other identity risk variable. If a change of address contributes to a risky identity pattern, this risk will likely result in a higher identity risk score which connotes higher risk.

To test whether identity risk scoring can predict ATO fraud, ID Analytics evaluated over two million consumer address changes, which occurred in a leading national credit portfolio. In this case, an identity-centric risk score was used to evaluate the risk of the address change information, based on the new address being requested. The results were very encouraging, with this approach effectively detecting ATO risk as follows:

- 41 percent of ATO accounts detected in riskiest scoring one percent of address changes.
- 32 percent of ATO losses detected in riskiest scoring one percent of address changes.
- Over $7MM in annualized ATO losses identified at one credit card issuer.

Just as identity risk scoring works very well for application fraud using ID Score, the same identity-centric approach showed superior performance in mitigating fraud for non-monetary events. Fully one-third of all account take-over losses in this case were identified by reviewing the riskiest scoring one percent of address changes.

Summary of Research Findings

Identity scoring offers a more effective approach to resolving address risk than traditional metrics such as area income level or distance moved.

- Conventional change of address wisdom is incorrect. Counter intuitively, high- to low-income moves are not the most risky income level move combinations.
- Changes in income level between areas are moderately predictive of identity risk, but over 90 percent of address changes do not involve changes in area income level.
- Moves within the same income level (high to high, medium to medium and low to low) are by far the lowest in terms of fraud risk, and make up the vast majority of change of address move combinations.
- Address changes of over 100 miles are more predictive of identity risk than income comparisons, but over 95 percent of consumer address changes occur between addresses less than 50 miles apart.
- The riskiest SCF to SCF moves are highly predictive of fraud risk, but the vast majority of reported moves are not risky.
- Identity risk scoring offers a comprehensive, highly predictive method to assess address risk with a third of all fraud identified in the highest scoring one percent of address changes.

Applying Identity Scoring to Identify ATO Cases

Figure 6 is a template for using identity-based scoring to vet address change risk. The score helps an organization fine tune the identity verification process. For very high scores with the highest ATO risk, an organization should immediately initiate investigations at the time of the address change. For moderately high-risk scores to highrisk scores, an organization may opt to initiate investigations when another high-risk event occurs in close proximity to the address change, such as a request for a new credit card or PIN. When an address change yields a low score, the organization categorizes the change as valid and eliminates costly reviews.

APPLYING IDENTITY SCORING TO ATO CASES

ADDRESS CHANGE SCORES	ATO RISK	RECOMMENDED ACTIONS
VERY HIGH	Highest ATO Risk	Initiate investigation at time of address change
MEDIUM/HIGH	Medium to High ATO Risk	Initiate investigation when other high risk actions occur (e.g. card/pin issuance)
LOW	Low ATO Risk	Eliminate investigations on low risk non-monetary events

Figure 6: Identity scoring can help organizations streamline the address change verification process

This approach both reduces fraud losses and the costs associated with reviewing low-risk address changes. Identity risk scoring can reduce operational costs of manual verifications stemming from compliance requirements by as much as 50 percent. For a large organization, this could mean a savings of over $1 million each year.

In addition to predicting the risk associated with an address change, ID Analytics' identity scoring approach also provides visibility into real-time address changes contributed to the ID Network® by ID Network Members. This is one of the earliest available sources of updates to an individual's identity information caused by life changes. The ID Network's visibility into these changes allows ID Analytics to better predict the risk of an address change.

It is particularly difficult for organizations to verify the risk of an address change during the consumer's first instance of an address change request. The first request is usually communicated to a utility, phone, cable or satellite TV provider. In these cases, traditional data matching is not viable because of the recency of this information, and organizations have come to understand that verification of addresses in isolation is not effective.

Federal Compliance

Identity risk scoring can also uniquely help organizations comply with the two new FACTA regulations relating to address discrepancies.

- **Resolving Address Discrepancies with a Credit Bureau:** Where there is an address discrepancy between a credit report and the address submitted on an inquiry, any user of the report must "form a reasonable belief that a consumer report relates to the consumer about whom it has requested the consumer report." In other words, the creditor must demonstrate that the credit report was retrieved for the correct identity.
- **Credit or Debit Card Address Changes:** FACTA also requires card issuers to evaluate the validity of an address change request made in close proximity to a request for a new credit card.

Where there is an address discrepancy with a credit bureau, identity scoring can automatically distinguish between benign address variations with low identity risk and those address variations where the risk to the identity is of concern. Similarly, identity scoring can determine if an address change on a credit or debit card account is not risky and therefore likely belongs to the applicant or account.

Conclusion

ID Analytics' technology is uniquely suited to understanding the identity risk associated with an address change because it can automatically distinguish between benign address variations with low identity risk and those address variations where the risk to the identity is of concern. ID Analytics identity-based scoring can be used to perform a rigorous and comprehensive analysis in order to determine to what degree, if any, an address discrepancy contributes to identity risk both at account opening and during on-going account management. Organizations can also use ID Analytics' technology to comply with regulations that mandate address change verification on certain transactions to prevent fraud.

For more information on ID Analytics identity intelligence solutions, please visit us at www.idanalytics.com or contact us at marketinginfo@idanalytics.com.

id:analytics®

www.idanalytics.com