Table of Contents

Introduction 3
What is Identity Fraud? 4
Types of Identity Fraud 4
What is an Identity Fraud Ring? 5
Examples of Fraud Rings 6
Where are the Identity Fraud Rings Located? 6
Fraud Trends 7
Summary 7
Introduction

According to a new study by ID Analytics’ ID:A Labs, there are more than 10,000 identity fraud rings in the U.S. This study is the first to systematically find many thousands of identity fraud rings, which was accomplished by developing an algorithm capable of automating the process of examining the interconnections between identity fraudsters to uncover rings of organized activity.

This automated approach represents a fundamentally important step forward in understanding and preventing identity fraud. In the past, ID Analytics’ research on fraud rings was conducted through manual spot checks and investigations of vast amounts of data, which uncovered a limited number of fraud rings. The company now for the first time employs a deterministic process for finding many thousands of identity fraud rings.

The study examined more than a billion applications for bankcards, wireless services and retail credit cards and found identity fraud rings attacking all three industries, with wireless carriers suffering from the most fraudulent activity. According to the study, Georgia, Florida and South Carolina are noted hotbeds of fraudulent activities across all three industries. The analysis is being used by ID Analytics to improve its identity fraud prevention and protection products and services.
What is Identity Fraud?

There are many different modes of fraud around identity and we classify and describe the majority of the common types. First, we define identity fraud:

Identity fraud is the act of misrepresenting which person you are in order to improperly obtain products or services.

Identity fraud occurs when one intentionally uses false personally identifying information (PII), in an attempt to represent himself as a different individual, who may or may not exist. It does not include misrepresenting or hiding behavioral characteristics such as past bad credit, but it does include pretending to be a different person to avoid past bad credit.

We make the distinction between mainline identity fraud and lost/stolen credit card fraud. While lost/stolen card fraud does include misrepresenting a particular person, this mode of identity fraud is limited to the use of that account only and ceases with the closing of that account.

Mainline identity fraud allows the fraudster to cause greater harm by using an individual’s PII such as name, Social Security number (SSN), and date of birth, to open multiple new accounts using the victim’s persona. This whitepaper deals primarily with mainline identity fraud. Note that our classification of identity fraud here is by fraud method and not by the industry or the personal demographics (e.g. age) being attacked.

Types of Identity Fraud

- **Lost/Stolen Account**: A fraudster becomes aware of enough information around a specific account that allows him to impersonate a victim for account-level activity. This manifests itself as unauthorized transactions such as credit card charges or possibly unauthorized money transfers. This type of fraud is limited to the account level and as mentioned above, is not generally considered mainline identity fraud.

- **Identity Theft**: A fraudster targets a specific real individual and assumes his persona. It typically manifests itself as unauthorized new account openings using the victim’s identity. In this mode of fraud, the imposter is aware that he is improperly representing himself as a specific, real person, whom he may or may not know personally.

- **Synthetic Identity Fraud**: A fraudster fabricates a new and false identity that is not related to a real person and does not actually exist. The perpetrator will invent a set of PII and try to establish the existence of this invented identity. This may be accomplished through the repeated presentation of this collection of fictitious PII on applications for credit, products and services across multiple channels and industries, with the intention of establishing this synthetic identity in the many existing credit-related databases to be misused at a later time. There may be some unintended overlap to real PII, however, the core identity is artificial.

- **Identity Manipulation**: A fraudster will make what may be slight and/or subtle variations to his true PII in the hopes of confusing the system to avoid having the application be associated with his true identity. The fraudster may increment one digit of his SSN, or month, day or year of his date of birth, or interchange SSN digits or otherwise manipulation his real PII in the attempt to confuse/disallow the application process to link this presented application to the fraudster. Identity manipulators may apply for products using slight variations of their true identity to attempt to avoid past delinquent history. Sex offenders and illegal immigrants commit identity manipulation to live under aliases to avoid detection, while other identity manipulators seek to gain improper access to health care or government services and benefits.
What is an Identity Fraud Ring?

Before we find and study these fraud rings we must define them:

*An identity fraud ring is a group of people actively collaborating to commit identity fraud.*

While some of these fraud rings are made up of what we might consider typical criminal “professionals,” many others are seemingly innocuous people and appear to be just like your friends and neighbors. These identity fraud rings can consist of family members or groups of friends. Family group rings that we observe may include parents, siblings, spouses, aunts and uncles, often using the same address and improperly sharing their PII. In some cases, a family group will bond with friends who have close family associations to increase the reach of their identity fraud activities.

**The Methodology**

ID Analytics operates the ID Network®, a cross-industry collaboration of data sharing for the purpose of identity fraud protection. This puts ID Analytics in a unique position to analyze risk events, such as new account openings or account changes, for the likelihood of identity fraud and credit risk. The company screens credit card openings, new cell phone account applications, new check orders, and other applications for many other products and services such as auto loans, installment credit and mortgages. Also screened are account-change events such as changes of address that can suggest attempts at account takeover. These hundreds of millions of events flow into the ID Network to give ID Analytics unique, real-time visibility into the dynamics of identity fraud and identity fraud rings.

Leveraging the data within ID Analytics’ ID Network, ID:A Labs looked at approximately 1.7 billion identity risk events, including these product applications, changes in PII among accounts such as changes in name, address, date of birth, and SSN, and other third-party data. The study examined this data in the ID Network from January 2009 to September 2012. Using in-depth research and analytics, ID:A Labs has found thousands of fraud rings operating throughout the U.S.

**About the ID Network**

The ID Network contains more than 700 billion instances of PII, like names, addresses, SSNs, DOBs, phone numbers and emails, providing visibility into more than 315 million unique people in the U.S. It has aggregated more than 1.7 billion consumer transactions that contain this PII, including 2.9 million reported fraud events, making the ID network the largest repository of reported fraudulent account opening events in the world. The bulk of the 1.7 billion consumer events are applications for new account openings, which allows ID Analytics to build tools for prevention of identity fraud, assessment of credit risk, authentication and compliance.

This vast quantity and quality of data has made it possible for the team at ID Analytics to uncover precisely where fraud rings operate, and on what industries they are focused. Through research, the company can determine if fraud rings are comprised of professional criminals, family members, or friends, and can identify the participants’ names, ages, locations and more. Following are some of the discoveries from this research.

**Identity Fraud Rings: Theft vs. Manipulation**

The rings may be either stealing victims’ identities or improperly sharing and manipulating their own PII such as their date-of-birth (DOB) and SSNs on applications for credit and services. We find identity fraud rings acting in both ways - some rings are only committing identity theft while other rings are only engaging in identity manipulation. Most identity fraud rings uncovered in the study are committing a blend of both identity theft and identity manipulation.
Examples of Fraud Rings

Following are examples showing the level of detail that can be exposed by analysis of data gathered from the ID Network. Please note that these stories are true and accurate, and to protect the privacy of individuals involved, only reveal a portion of what has been discovered about these individual fraud rings.

- **Fraud Ring #1:** A friends-and-family identity fraud ring that consists of a male and female over the age of 70, a woman of 48 with the same family name, and a second woman of 48 with a different last name. All participants are using multiple SSNs and last names; three have alternate first names and birthdates. Together, this identity fraud ring has perpetuated 345 falsified credit card applications and a fraudulent payday loan. The male is retired, but uses a former email address from a respected institution to increase credibility. This fraud ring is located in a subdivision in the Indianapolis area.

- **Fraud Ring #2:** This family-and-friends identity fraud ring has six participants and is located in an apartment complex in Washington DC. From the ages and names observed by the ID Network, the group appears to be led by a 52-year-old woman and her sister, joined by three 20-something daughters and a likely boyfriend. Together this team has used ten SSNs and multiple first names, last names and birthdates to commit fraud. In addition to identity manipulation, this group is also applying for accounts using stolen identities (identity theft). They have completed more than 69 credit card applications and defrauded four victims, including two deceased persons.

- **Fraud Ring #3:** Another family-and-friends team, this group appears to be comprised of two family groups operating from nearby homes in McAllen, Texas. There are eight members in the ring, ranging from 19 to 53 years of age. Together they have submitted 142 felonious applications from two addresses, with two members (who improperly share SSNs and phone numbers) primarily targeting wireless providers. Two other members are focused on retail credit and bankcards, and, perhaps not surprisingly, it appears that the children in the group are stealing their own parents’ identities. Four unrelated persons’ identities have also been stolen. This fraud ring is also combining identity manipulation and identity theft.

Where are the Identity Fraud Rings Located?

ID Analytics research pinpoints the exact locations of where these rings are operating. Although fraudsters can be found anywhere in the U.S., there appears to be a “belt of fraud” that runs through the rural Southeast, extending from Virginia to Mississippi, with significant activity in the Carolinas, Georgia, Florida and Alabama. There are also hot spots of fraud ring activity in Louisiana, Texas, New Mexico, Arizona and the West Coast. We find further hotbeds in Michigan, Delaware, Kentucky, Tennessee and Arkansas.

ID Analytics examined smaller regions within states that have high levels of identity fraud ring activity. The top three-digit ZIP codes where fraud ring activity was observed include regions around Washington DC; Tampa, Fla.; Greenville, Miss.; Macon, Ga.; Detroit; and Montgomery, Ala.

Fraud rings can be found anywhere in the U.S., but research shows a belt of fraud stretching through the rural Southeast.
Fraud Trends

Targeting the Deceased
Fraudsters can be devious and will leave no stone unturned. One type of identity fraud involves targeting and stealing the identities of dead people. Through various means, fraudsters gather the PII from people whom they know are deceased and use that information to open new credit card accounts and make purchases. When the bill comes due, there is no responsible party.

Credit Mules
Another emerging fraud trend which is not identity fraud is that of “credit muling,” which involves paying a person to use their legitimate PII with the intention to defraud. Note that this is not really identity fraud since the applicant is using only their correct identity information; it’s just that they have no intention to repay the debt. This technique is becoming more frequent with wireless customers who have previously earned a decent credit rating. A fraudster hires such a person, known as a credit mule, to visit a wireless store and open a new account in their true name. The mule then purchases several new phones in original packaging, with no intention of paying when the bill comes due. The fraudster (often waiting outside) then buys the phones for cash from the mule, which he will then resell into the international market where the phones may not yet be released or are hard to attain, at a high rate of return. The credit mule is either unaware or is not concerned that his or her credit rating will suffer—the mule is just looking for fast cash.

Summary
The ID Analytics study revealed the existence of over 10,000 identity fraud rings through a systematic ring discovery process. Surprisingly, although it’s often assumed that professionals are the masterminds behind identity fraud rings, a large number of fraud rings consist of small groups of family and/or friends. Among that group, many families are working together in fraud rings, using each other’s SSNs and dates of birth, as well as committing a combination of identity theft (stealing someone’s identity) and identity manipulation (improperly modifying their own PII).

ID Analytics also found that these criminals are most likely to target three main industries, focusing on the bankcard, wireless and retail card industries, with wireless carriers suffering from the most fraudulent activity.

Although they can be found throughout the U.S., the study indicates that there are distinct hotbeds for fraud rings, as evidenced by the included U.S. map that reveals a belt of fraud extending from Virginia, through the Carolinas, across Georgia and Florida, reaching Alabama and Mississippi. And, while many fraud rings operate in cities, a surprisingly high number of rings operate in rural areas as well.

ID Analytics solutions protect you and your clients
Partner with an experienced, trusted firm. Since 2002, ID Analytics has been delivering a unique perspective of risk based on proprietary Advanced Analytics and the ID Network®, one of the nation’s largest networks of cross-industry consumer behavioral data, data not available in consumer credit reports. For more information about ID Analytics contact us at marketinginfo@idanalytics.com or 858-312-6200 or visit www.idanalytics.com.

ID Analytics is a registered trademark of ID Analytics, Inc. All other trademarks and registered trademarks are the property of their respective holders.