# New Application Reveals Where Your Identity is Being Used Today

## Reduce Your Risk of Being Breached by Identity Thieves and Cyber Criminals

### Presented by Secure Identity Systems

### Introduction

The face of identity theft is always changing and getting smarter. It's a scary fact, but new fraud victims are found every two seconds. Are you ready to deal with the next level of identity theft?

Unfortunately, no one is safe from identity theft.

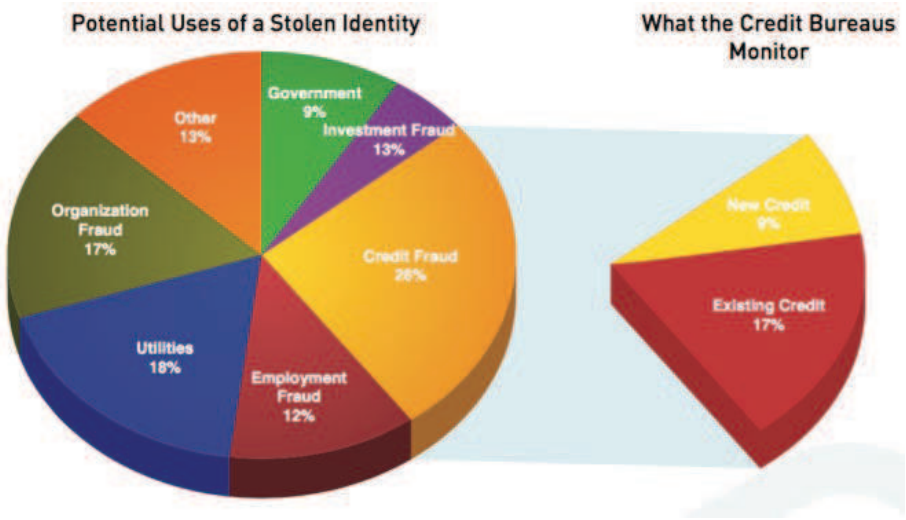
- The U.S. Department of Justice estimates 17.6 million individuals, or 7% of all U.S. residents age 16 or older, were victims of one or more incidents of identity theft in 2014.
- A survey that Secure Identity Systems commissioned found that 35% of bank customers are only somewhat or not at all confident that their personal information is secure at their financial institution.
- A Gallup poll found that the biggest worry for consumers is identity theft, causing concern for nearly 70% of respondents.
- 57% of banking customers surveyed by Secure Identity Systems responded that they would be at least somewhat likely to switch to another bank if free identity theft protection services were offered.
- Only two-thirds of identity fraud victims are notified of a data breach, a 2015 Javelin study found.

The face of identity theft is always changing—and it's getting smarter. Identity theft protection is of the upmost importance to your customers, but it's not all gloom and doom for financial companies and individuals. Now more than ever before, we have an opportunity to amp up security practices to combat the next level of identity theft and catch illegal use of identities.

### Total Identity Monitoring

The belief that credit monitoring alone will keep your identity safe is like believing that if you only lock one of your car doors the purse sitting on the front seat will be safe. To catch an identity thief, it is not enough to monitor your credit report.

According to the Federal Trade Commission (FTC), 70% of identity theft is non-credit related. Ask a layperson why someone would want to steal his or her identity and he or she will guess credit card fraud. But, the FTC statistics show that only 26% of stolen identities are used for credit fraud.



Thieves use your identity for all kinds of reasons that are not credit related. For example,

- Illegal aliens may buy a stolen identity of get a job
- A sex offender may be living in an area he isn't allowed under your name
- Firearms can be purchased, used and found at a crime scene
- Drivers License information can be used in a DUI charge now on your record
- Utility accounts may be opened and left unpaid
- Tax returns can be filed under your name

To catch these types of identity thieves, in addition to credit monitoring, you need to monitor databases that reach all verticals of life. Secure Identity Systems monitors over 1,000 databases including Social Security, driver's license, utilities, call centers, credit account applications, demand deposit accounts (DDA), brokerage accounts, insurance, Web environments and more. Security solutions that offer narrowly focused identity theft monitoring products in specific categories — court/criminal, utilities, payday loans, etc. — are not enough, and combining several products to get the coverage you need can get very expensive.

You can find an in-depth look at database monitoring in the Resources section of this whitepaper.

## How Total Identity Monitoring Works

When an individual enters his or her information, the system returns an identity theft risk level:
Green (low): System did not find concerning information
Yellow (medium): Recovery advocate assists in further investigating the scan
Red (high): Recovery advocate thoroughly reviews and creates a recovery plan with customer

## Have You Had Your Data Held Hostage Before?

"It was attempted. It was a virus and [the hackers] wanted me to pay $400 to unlock. I was able to get into the System BIOS and get the computer booted and restore a previous version." —
Greg Luken, CEO, Luken, Financial Services Industry

## Recovery

When identity theft strikes, the amount of paperwork and time it takes to clear up the identity can be overwhelming. Many victims don't know where to turn for help. According to the FTC, it can take a victim between 60-600 hours to repair damage caused by identity theft. Victims suffer not only damage to their good name, but also stress and expense — often in the thousands of dollars — trying to put their credit and life back together.

If you invest in an identity theft "Recovery Advocate," you'll have someone who can do the repair work for you. Being able to find your identity when it's missing is like being able to find your phone when it's missing — it's truly a life-saving tether.

**The Recovery Process**

When an individual reports his or her identity theft, a Recovery Advocate develops a personalized recovery plan that is based on the damage assessment. The Advocate then obtains reports from the three credit reporting agencies and performs extensive database searches to determine the extent of the fraud, and works with these agencies and local law enforcement to completely restore the victim's identity to pre-event status.

For the more complex cases, the Advocate consults with legal consultants and forensic accounting specialists and fraud investigation team made up of former FBI and other law enforcement officials. Lastly, the Advocate provides post-recovery follow-up for 12 months to assure no further problems have surfaced.

## POS Intrusions Compromise Hospitality, Entertainment & Retail Industries

In 2014, the evolution of attacks against point-of-sale (POS) systems continued, with large organizations suffering breaches alongside small retailers and restaurants. Large breaches tended to be multi-step attacks with some secondary system being breached before attacking the POS system.

(Source: Verizon's 2015 Data Breach Investigations Report)

## Reimbursement

Recovering one's identity can be expensive. In 2014, 65% of identity theft victims reported a combined direct and indirect financial loss, according to the U.S. Department of Justice's Victims of Identity Theft report. These losses include the direct financial loss of any monetary amount stolen as well as other costs caused by the identity theft, such as legal fees, bounced checks and other miscellaneous expenses (e.g., postage, phone calls, or notary fees). Victims who experienced a direct and indirect financial loss of at least $1 lost an average of $1,343.

Most identity theft Expense Reimbursement Programs are very limited or have high deductibles or fine print clauses that make any reimbursement next to impossible. Most also do not include lost wage reimbursement for the self-employed. When working with a third-party security vendor to set up an Expense Reimbursement Plan, make sure you read the find print and fully understand the benefits you are entitled to in case of a breach.

## EMV Credit Card Chip Conversion

In October 2015, the Europay, MasterCard and Visa (EMV) chip-and-pin mandate went into full effect in the U.S. This should decrease instances of card-present fraud, but before you get too excited, the decrease of card-present fraud will likely be offset by an increase card-not-present/online transaction fraud.

## Reimbursement

Cyber-crime losses are just as hefty for businesses. Verizon's 2015 Data Breach Investigations Report found with 95% confidence that the average loss for a breach of 1,000 records to be between $52,000-$87,000. Larger organizations have higher losses per breach, and they typically lose more records and have higher overall costs.

Cyber-crime is not covered by general business liability insurance, but it is relatively inexpensive and can save your organization thousands of dollars in future fees and expenses. Think of it this way: adding the expense of a new insurance premium is never going to shut down your business, but suffering a breach without insurance might do just that. According to Ponemon Institute's Third Annual Data Breach Study, 25% of organizations are currently covered by cyber insurance, and 35% of respondents say their organizations plan to purchase cyber insurance within the next year.

Most cyber-crime insurance covers notification in the event of a loss of protected information, crisis management costs to restore customer confidence, and regulatory fines and penalties and credit monitoring expenses for victims of the breach.

## Conclusion

Nowadays, it's not a matter of if your business will be breached or if your identity will be stolen, but when. You can combat this hard truth by employing the tactics discussed in this white paper. As we innovate our identity theft security measures, adversaries will also be innovating and quickening their hacks. As daunting as the challenge seems, sitting back and watching is not an option for the good guys. While we cannot eliminate all the bad players out there, but we can play smart and make ourselves the most difficult possible target for cyber criminals and identity thieves.

## Resources

Database Monitoring
Total Identity Monitoring provides the most comprehensive level of monitoring of more than 1,000 public and non-public data sources. By searching for anomalies within this matrix of information, you can detect fraudulent activity that you wouldn't find with a standard credit check.

Individual
SSN, DOB, Address Histories, Phone, Aliases, Relative and Associates, Voter's Registration

Federal and State License Filings
Education, DEA, Professional, Driver's License, Hunting & Fishing, Pilots, Concealed Weapons

Financial & Business
Credit Applications, National File with Proprietary Databases, Dun & Bradstreet, Domain Registration, Death Benefits, Tax Returns, Social Security Benefits

Assets
National Property, Vehicles, Boats, Aircraft, Recreational, Merchant Vessels

Reputation
Office of Foreign Assets Control (OFAC), Blacklists and Fraud Alerts, High Risk Alerts, Court Records, Bankruptcies, Judgments, Liens, Associates

**About Secure Identity Systems**

Secure Identity Systems was initially created to mitigate the risk for financial institutions by identifying growing security threats. By 2006, Secure Identity Systems held three North American Patent Rights for ID Theft prevention and authentication. By the time the regulatory “Joint Release Red Flag Rule” was handed down, SIS was the only company in the U.S. to have a complete end-to-end solution already in place. Today, SIS serves financial institutions, businesses and families with the most robust products and services available.

For more information on Secure Identity Systems, please call 877.304.3349 or visit SecureIdentitySystems.com. Follow Secure Identity System on Facebook and Twitter for security updates and special offers.