INTRODUCTION

Welcome to the CSID Marketing Toolkit.

As our valued partner, we want to help you bring your identity protection products to market easily and successfully. We created this document is to provide you with content, tips and information that will assist in the positioning and messaging of the products CSID is powering for you. This Toolkit includes:

- CSID product information, benefits and consumer facing value propositions
- Online marketing best practices geared toward an identity protection and fraud detection product.
- General and vertical-specific industry statistics

Please keep in mind as you review this document that it is written in your voice, in an attempt to add value to your marketing efforts.

Should you have any questions about this document, please contact us at marketing@csid.com.

Table of Contents

INTRODUCTION **1**

CSID PRODUCTS **5**

PRODUCT SUMMARY 5

CREDIT 6

Credit Reporting and Monitoring *6*

Score Plotter *7*

COMPREHENSIVE IDENTITY 7

CyberAgent® *7*

Bank Account Takeover Monitoring and Credit Card Application Monitoring** *9*

Social Media Monitoring *9*

Social Security Number Trace *10*

Court Records and Bookings Monitoring *11*

Non-Credit Loan Monitoring *12*

Sex Offender Monitoring *13*

Change of Address Monitoring *13*

RESTORATION 14

Identity Restoration *14*

Lost Wallet *15*

Identity Theft Insurance *15*

MARKETING BEST PRACTICES **17**

CREATING NEED FOR AN IDENTITY PROTECTION PRODUCT 17

CSID POWERED MESSAGING 17

INDUSTRY-SPECIFIC MESSAGING 17

Financial *17*

Insurance *18*

Gaming *18*

Government *19*

Healthcare *19*

Telecommunications *19*

Online/ecommerce *20*

Consumer *20*

ONLINE MARKETING VEHICLES 21

Search Engine Optimization (SEO) *21*

Search Engine Marketing (SEM) *21*

Social Media *22*

Social Advertising *22*

Email Marketing *22*

Online Advertising *23*

OTHER MARKETING TACTICS 23

Testimonials *23*

Blog *23*

Case Studies *24*

Videos *25*
Frequently Asked Questions (FAQ) *25*

IDENTITY THEFT STATISTICS **26**
FRAUD IN THE UNITED STATES 26
Key Messages *26*
Supporting Messages *26*
GLOBAL FRAUD 27
ID THEFT 28
CHILD ID THEFT 28
Key Messages *28*
Supporting Messages *29*
DATA BREACHES 30
Key Messages *30*
SUPPORTING MESSAGES 31
IDENTITY FRAUD LIFECYCLE 32
Key Messages *32*
Supporting Messages *32*
COST OF FRAUD 33
Key Messages *33*
PASSWORD MANAGEMENT 33
Key Messages *33*
Supporting Messages *34*
CONSUMER PROFILES 34
Key Messages *34*
Supporting Messages *35*

INDUSTRY- SPECIFIC STATISTICS **35**
FINANCIAL 35
BUSINESS 36
EDUCATION 36
GOVERNMENT 37
HEALTHCARE 37
TELECOMMUNICATIONS 38
ONLINE/E-COMMERCE 39

FREQUENTLY ASKED QUESTIONS **39**
GENERAL QUESTIONS 39
IDENTITY THEFT QUESTIONS 41
CREDIT QUESTIONS 44
Credit Monitoring *44*
Credit Reports *44*
Score Plotter *44*
COMPREHENSIVE IDENTITY QUESTIONS 45
CyberAgent® *45*
Social Security Number Trace *46*
Court Records Monitoring *46*
Non-Credit Loan Monitoring *47*

Sex Offender Monitoring *47*
Change of Address Monitoring *48*
Self-Service Restoration *48*
Insurance *49*
Lost Wallet *49*

CSID PRODUCTS

Product Summary

Credit Reports and Scores	Single or tri-bureau credit reports and scores
Credit Monitoring	Monitors one or all three bureaus for inquiries, delinquencies and more
Score Plotter	A widget that plots single or tri-bureau credit scores on a chart so that individuals can easily see trends over time
CyberAgent	CyberAgent that scours websites, blogs, bulletin boards, peer-to-peer sharing networks and IRC chat rooms
Bank Account Takeover Monitoring*	Notifies users when their SSN and personal information have been used to open a new bank account or if changes have been made to their existing bank account
Credit Card Application Monitoring*	Notifies users if their SSN and personal information have been used to apply or open a new credit card account
Child Monitoring	Checks and notifies when fraudulent names, aliases and addresses become associated with the SSN of a minor
SSN Trace	Provides users with a report of all names and aliases associated with their SSN, and notifies them if a new one is added
Social Media Monitoring	Watches your social media activity and notifies you of privacy or reputation risks with the content you are sharing.
Court Records Monitoring	Tracks municipal court systems and alerts customers if a criminal act is committed under their names in real time
Bookings Monitoring	Tracks bookings data from law enforcement agencies to find any criminal offenses under a customer's name and date of birth
Non-Credit Loan Monitoring	Alerts users if a Payday loan has been opened using an element of an their identity
Change of Address Monitoring	Reports if an individual's mail has been redirected though the US Postal Service
Sex Offender Monitoring	Provides a report of all registered Sex Offenders living within a defined radius of a user's zip code, and alerts the user when a new Sex Offender is added. It also notifies users if a Sex Offender fraudulently registers using his or her identity elements
Lost Wallet	Assists members in quickly and effectively terminating and re-ordering wallet contents. Users are not required to pre-register wallet contents before using this service.
Identity Restoration	Gives users access to a restoration specialist to offer tips, detailed instructions and follow-up to assist members in restoring their identity. Varying levels of coverage are available.

$1M Insurance	Covers costs associated with identity restoration for up to $1M with $0 deductible

*Note: Bank Account Takeover Monitoring and Credit Card Application Monitoring are both elements of a singular service offered by CSID – Financial Account Takeover.

Credit

Credit Reporting and Monitoring

Provides users with single or tri-bureau credit reports, scores and monitoring.

Benefits:

- Credit monitoring provides you with notifications for changes in a credit report such as loan data, inquiries, new accounts, judgments, liens and more.
- Tri-bureau reports are available from all three major credit reporting agencies, allowing you to proactively manage your financial health and monitor your identity.
- Tri-bureau credit reports provide credit scores and corresponding score factors (such as accounts in delinquency or new accounts opened), and rankings on where you stand in relation to other individuals
- When you know your credit score, you have access to the same criteria that banks, lenders, and even employers use in evaluating credit worthiness
- Opening up lines of credit is a very common and costly form of identity theft, and monitoring your credit is the fastest and simplest way to guard against fraudulent activity taking place under your identity

What is Credit Monitoring?
Credit Monitoring includes monitoring of changes reported to all three national credit bureaus (Experian, Equifax and TransUnion). Changes monitored include personal information, public records, inquiries, new account openings, and existing accounts reported past due.

What should I do if I receive a notification for something that didn't happen?
In some cases, the credit-reporting agency may commit errors on your credit file and the incorrect information may trigger a notification. Nevertheless, if you see a credit notification that is not accurate; please contact customer support.

How often is my credit monitored?
Credit bureau notifications are generated through consistent monitoring, and are distributed multiple times a day. A credit bureau file is monitored daily and any notifications triggered as a result of new inquiries and/or adjustments made to a credit file are sent to you via email.

What should I do if I see a mistake on my credit report?
In some cases, the credit-reporting agency may commit errors on your report - the incorrect information may simply be a mistake. However, an error on your credit report could indicate that an identity theft event has occurred. If you see incorrect information on your credit report, please contact customer support.

Why is there a difference between my three scores?
Each credit-reporting agency generates a score derived from what is reported about you. A creditor may report to one, two or all three of the national credit bureaus. As a result, the information one credit bureau has may be different than another, resulting in a different credit score.

What time range does my initial credit report cover?
Your credit report includes data beginning from the date your credit file was first established. This could span more than 25 years.

Score Plotter

A widget that initially plots your tri-bureau credit scores on a graph, and then charts your TransUnion credit score month-over-month so that you can easily see trends over time.

Benefits:

- An intuitive graph that displays the change in your credit score over time, giving you more control over your financial health
- Track how your credit score changes over time for ongoing insight into your credit health
- View your credit score regularly, without having to incur extra cost by pulling a full credit report

What does it mean if I see big changes in my credit score from month to month?
Every reported item on your credit report is used to calculate your credit score. If your score has changed significantly since the last month, it may be due to the fact that an account was not reported for the month or an item has been added to or removed from your report. Drastic changes in account balances and opening new lines of credit could also significantly impact your score.

How many months does Score Plotter show me?
Score Plotter plots your credit score for past 12 months.

Is the credit score that Score Plotter plots related to a specific bureau?
Yes. Score Plotter plots your TransUnion credit score.

Comprehensive Identity

CyberAgent®

CyberAgent scours Internet properties like websites, blogs, bulletin boards, peer-to-peer sharing networks and IRC chat rooms to identify the illegal trading and selling of your personal information. At any point in time, this technology is monitoring thousands of websites and millions of data points, alerting you if your personal information is found being bought or sold online.

Benefits:

- CyberAgent proactively detects stolen PII, alerting businesses and giving them the opportunity to stop the leak early, get ahead of potential bad press and take proactive steps to protect their customers and employees.
- CyberAgent is the only identity monitoring solution designed for data collection on an international level, regardless of a country's credit system or language
- At any point and time, our CyberAgent technology is monitoring thousands of websites and millions of data points, alerting consumers if we find their personal information in a compromised position online
- This information is being gathered in real-time giving both businesses and consumers the opportunity to react quickly and take the necessary steps to protect themselves

What information do I enter in the Medical Identities field?
Enter your Member ID number as it appears on your health insurance card.

Where does CyberAgent data come from?
This data comes from Internet forums and websites, web pages, IRC channels, refined PII search engine queries, Twitter feeds, P2P sources, hidden and anonymous web services, malware samples, botnets, and torrent sources.

What time range does my initial CyberAgent report cover?
Your first CyberAgent report includes data from the previous 8 years. This means that our tool searches the prior 8 years of records it has collected for a match to the personal information you are monitoring.

What does it mean when I receive an alert?
Your CyberAgent service tracks Internet activity for signs that the personal information you've asked us to monitor is being traded and/or sold online. This notification means that our surveillance technology has discovered information on the Internet that is a match to your monitored identity elements.

What if the notification references only some of the personal information CyberAgent is tracking?
Even if only some of your personal information that has been detected by CyberAgent, it is recommended that you contact the appropriate institution to have your account information changed, or change your account information yourself if possible - like it would be with the password to your email account. It is safe to assume that if some of your information is compromised, all of it is. You may also want to review a copy of your credit report to ensure that all of the information that appears there is familiar to you.

Is the buying and selling of others' personal information online illegal?
This activity is illegal in the United States, but other countries do not necessarily have the same laws as related to cyber crime. United States regulatory agencies have no jurisdiction to prosecute fraudsters acting on websites and chat rooms located in other countries.

Can I still become a victim of identity theft even though I am enrolled in CyberAgent?
CyberAgent dramatically reduces your risk of identity theft by letting you know sooner if your personal information is compromised, and in turn enabling prevention or quick resolution of an identity theft incident. In addition to CyberAgent, you also have identity protection insurance and recovery services to help alleviate some of the financial burden of identity theft and guide you through the often confusing and difficult process. Unfortunately, no identity protection tool can prevent identity theft altogether.

Bank Account Takeover Monitoring* and Credit Card Application Monitoring*

*Note: Bank Account Takeover Monitoring and Credit Card Application Monitoring are both elements of a singular service offered by CSID – Financial Account Takeover.

Financial Account Takeover notifies you if your Social Security number and personal information have been used to open a new bank account; or if changes have been made to your existing bank account, including changes to account contact information or attempts to add new account holders. Also notifies you if your Social Security number and personal information have been used to apply or open a new credit card, checking or savings account.

Benefits:

- Provides early detection of suspicious banking or credit card account activity and possible identity fraud
- Reviews information contributed daily from hundreds of financial institutions to flag unusual or high-risk account activity.
- Reduces the time, money and emotional stress associated with a compromised bank account or fraudulent bank or credit card account

What records does Financial Account Takeover search for my personal information?
This service monitors your personal information against transactions from hundreds of financial institutions across all 50 states, including:

- Broad monitoring network, including the top 10 regional banks and credit unions
- Bank of America, BB&T, Capitol One, JPMorgan Chase, and Wells Fargo
- Visa and MasterCard
- 49.6 million new credit and demand deposit accounts new inquires annually

What is Financial Account Takeover monitoring, and how soon will I receive a notification if my personal information is found compromised?
This service monitors your name and SSN, and will notify you daily if unusual or high-risk activity is detected. If detected, you will receive the following notifications:

- **New Bank Account Opening Notification**– If your personal information has been used to open a new bank account
- **Bank Account Takeover Notification**– If changes have been made to your existing bank account, including changes to account contact information or attempts to add new account holders
- **Credit Card Application Notification**– If your personal information has been used to apply for a new credit card
- **Credit Card Opening Notification**– If your personal information has been used to open a new credit card account
- **Checking or Savings Account Application Notification**– If your personal information has been used to apply for a new checking or savings account

Social Media Monitoring

Social Media Monitoring watches your social media activity and notifies you of privacy or reputation risks.

Benefits:

- Searches for instances where your personal information is exposed via social sites – profile info, comments, wall posts and more – and notify of these privacy risks.
- Notifies you of content on your social networks that may damage your reputation like foul language, sexual content, and drug and alcohol references.

What social networks does Social Media Monitoring track?
The service tracks Facebook, Twitter, LinkedIn and Instagram.

Can I add more than one account for any social network?
No, only one account per network can be monitored at this time.

How far back does my initial report search?
45 days

How soon after risky content is posted will I be notified?
You will receive a notification within 24-48 hours.

Does this service scan my images in addition to the written content posted on my social networks?
Social Media Monitoring does not currently scan images, but it does scan the image caption or post that goes along with it.

Social Security Number Trace

Provides you with a report of all names and aliases associated with your Social Security number, and notifies you if a new one is added.

Benefits:

- Helps you detect identity theft sooner
- Enables you to have greater intelligence regarding how your SSN is being used
- Greatly reduces the time, money and emotional stress associated with a stolen SSN

What do I do if there is a name or address in the Social Security Number Trace report that I don't recognize?
If your report contains names and/or addresses that are not familiar to you, there is probably an error in public records information. However, this could be an indication of identity theft. If you see unfamiliar information in your Social Security Number Trace report, please contact customer support.

What do I do if an old address is incorrect in the Social Security Number Trace report?
It is not uncommon for address history dating back more than 5 years to contain errors. However, if the incorrect address is more recent, please contact customer support.

What do I do if I see a name on the Social Security Number Trace report or notification that isn't my current name?

It's not uncommon to see alternate names on your report due to marriage, joint credit accounts and nicknames you may have used. However, if you are concerned, please contact customer support.

What time range does my initial Social Security Number Trace report cover?
Your first Social Security Number Trace report looks at data beginning from the date your SSN first entered public records. This could be as early as when you were born and issued an SSN.

Court Records and Bookings Monitoring

Tracks municipal court systems and notifications you if a criminal act is committed under your name in real time, as well as bookings data from law enforcements agencies to find any criminal offenses under your name and date of birth.

Benefits:

- Helps you detect if your PII has been used by identity thieves with law enforcement to avoid embarrassing and damaging legal incidents
- Receive monthly monitoring and notifications when the changes to your report are discovered, based on first name, last name, address, date of birth or offense
- Receive monitoring notifications within 24-48 hours from the time a booking occurred

Why doesn't my Court Records and Bookings Monitoring report have any information in it?
This is usually a good thing! It means that we didn't find a match to your personal information in our court records data. This may be due to one of the following:

- You have never been convicted of a crime
- Your identity has not been stolen for the purpose of committing a crime
- Your court records have been expunged or your court records have not yet been updated in the public records database

What records does Court Records and Bookings Monitoring search for my personal information?
Court Records and Bookings Monitoring searches court records and bookings data sourced from the following places:

- Over 509 million criminal court records mapping to federal, state, city, and county level jurisdictions
- Over 60 million incarceration records spread across 2,100 police organizations covering over 70% of national bookings
- 99 million Department of Corrections (DOC) parole, probation, and incarceration records
- Over 4.9 million warrant records. 98 county, state and city level warrants reporting 664 of 3,248 counties in 50 states and Puerto Rico
- Over 9 million arrest records
- Over 330 thousand government records, such as Most Wanted and terrorist lists

Does Court Records and Bookings Monitoring report on records from all states and counties?
No. Court records data restricted states and territories include Maine, Wyoming, South Dakota, District of Columbia, and Puerto Rico. Department of Corrections data restricted states include Arkansas, Colorado, District of Columbia, Delaware, Hawaii, Massachusetts, South Dakota, Virginia, Washington and Wyoming. Bookings data restricted states and territories include Arkansas, District of Columbia,

Delaware, Hawaii, Kansas, Massachusetts, Maine, Montana, North Dakota, Nebraska, New Hampshire, Pennsylvania, Puerto Rico, South Dakota, Vermont, Washington, and Puerto Rico.

What if I see court records in the report that aren't mine?
False matches in court records report can occur as a result of an individual having the same name and/or date of birth as you. This can usually be resolved by calling the relevant courthouse to make sure the records belong to another individual. If the courthouse confirms that the records in question relate to your identity – usually done by confirming your SSN or driver's license number – and you did not commit the infraction, you may be a victim of identity theft. If you are concerned, please contact customer support.

How soon will I receive a notification after a new court record is entered or a booking incident occurs?
You should see a notification within a month from the date a new court record is entered.

What time range does my initial Court Records and Bookings Monitoring report cover?
Your first Court Records Monitoring report includes court and bookings data from the past 10 years.

What if I see see bookings data that isn't mine?
False matches in court records report can occur as a result of an individual having the same name and/or date of birth as you. This can usually be resolved by calling the relevant courthouse to make sure the records belong to another individual. If the courthouse confirms that the records in question relate to your identity – usually done by confirming your SSN or driver's license number – and you did not commit the infraction, you may be a victim of identity theft. If you are concerned, please contact customer support.

How soon will I receive a notification after a new court record is entered or a booking incident occurs?
You should see a notification within 48 hours from the time a booking incident occurred.

Non-Credit Loan Monitoring

Notifies you if a non-credit loan has been opening using an element of your identity.

Benefits:

- Monitor the transactions associated with non-credit or payday loans to detect fraud where credit monitoring alone cannot
- Have peace-of-mind with comprehensive identity theft protection
- Understand if you have been a victim of non-credit/payday loan fraud earlier to minimize restoration time and headache

What is a non-credit loan?
Non-credit loans include both payday and quick-cash loans that do not require a SSN or credit inquiry to complete. Non-Credit Loan Monitoring notifications users if this type of loan has been opened using an element of their identity.

How many non-credit loan establishments does Non-Credit Loan Monitoring report cover?
Non-Credit Loan Monitoring gets data from 23 of the top 25 payday lenders.

What time range does my initial Non-Credit Loan Monitoring report cover?
Your first Non-Credit Loan Monitoring report includes data from the past 2 years.

Sex Offender Monitoring

Provides a report of all registered sex offenders living within your immediate area, and notifications you when a new sex offender is added. It also notifies you if a sex offender fraudulently registers using your identity elements.

Benefits:

- Become familiar with the sex offenders that live in your neighborhood
- Know where sex offenders live so you can make more informed decisions regarding where you move, send your children to school and allow your family to spend time
- Gain more control over the health and safety of their family when it comes to sex offenders
- Ensure a sex offender does not steal your identity to register

What records does Sex Offender Monitoring search for my personal information?
Sex offender records are generated from entries in the national sex offender Registry (SOR). Sex Offender Monitoring searches a database of over 1.8 million records from 49 state registries as well as Washington DC, Native American reservations, Guam, Puerto Rico, and the US Virgin Islands. Mississippi does not allow access to its records, but information about sex offenders in this state are still included in our database when offenders have moved there from other states.

Are all sex offenders required to register in the national SOR?
Not all criminals convicted of a sex-related offense are required to register with the SOR. The SOR includes only those offenders who were ordered to register via a criminal court case in their jurisdiction. Sex offenders who were not ordered to register with the SOR would still appear in a criminal records database, and could have an offense description indicating a sex crime.

What if I see my name used by an offender in the Sex Offender Monitoring report?
False matches in this report can occur as a result of an individual having the same name and/or date of birth as you. This may also indicate that a sex offender has used your name or personal information to register.

A false match can usually be resolved by calling the relevant courthouse to make sure the records in question belong to another individual. If the courthouse confirms that the records in question relate to your identity – usually done by confirming your SSN or driver's license number – and you have not been convicted of a sex crime, you may be a victim of identity theft. If you are concerned, please contact customer support.

How often is my Sex Offender Monitoring report updated?
Your Sex Offender Monitoring report is updated monthly. If there is a change in the data returned at this time, you will receive a notification.

Change of Address Monitoring

Reports is your mail has been redirected through the U.S. Postal Service.

Benefits:

- Be alerted if someone tries to steal your identity by redirecting your mail to a new address
- Note that it can take up to 2 weeks for the USPS to process a change of address request

Where does Change of Address Monitoring data come from?
Change of Address Monitoring report only changes in address that have been processed through the United States Postal Service (USPS). Change of Address Monitoring does not track UPS or FedEx-only addresses or private mailboxes.

How long after I submit a change of address request will I receive an alert?
The USPS can take up to two weeks after the "effective date" to publish the address change. You will receive a notification once the change has been published.

What do I do if there is an address in Change of Address Monitoring that I don't recognize?
If your report contains an address that is not familiar to you, there is probably an error in public records information. However, this could be an indication of identity theft. If you see unfamiliar information in Change of Address Monitoring, please contact customer support.

What time range does my initial Mail Change report cover?
Your first report includes data from the past 3 months, including the current month.

Restoration

Identity Restoration

Full Service Identity Restoration by CITRMS (Certified Identity Theft Risk Management Specialist) designated staff reduces the time and effort a member endures in the event that their identity is stolen, and goes beyond traditional credit report restoration by offering robust cast knowledge in non-credit restoration.

Benefits:

- Supports members in restoring their identity in the event their identity is compromised
- Offers bilingual specialists, multilingual and hearing-impaired services are offered 24-hours a day, 7-days a week
- Includes Limited Power of Attorney so that the specialist assigned to your case can truly complete all restoration activities on your behalf
- Delivers value when members need it most and protects individuals in the event of identity theft

How will being enrolled in ID Notify help me restore my identity if I become a victim of identity theft?
As specialists, we'll help you determine if an identity theft event has occurred and guide you through any necessary restoration activities. We may take the following actions on your behalf:

- Contact your issuer or banking institution
- File a police report
- Review your credit report for indications of identity theft
- Place a fraud notification or security freeze with the three credit bureaus

Lost Wallet

Assists you in quickly and efficiently terminating and re-ordering wallet contents. You are not required to pre-register wallet contents before using this service.

Benefits:

- Enables you to quickly and safely address a lost wallet without preregistering wallet contents
- Saves you time and stress by working on your behalf to cancel and re-issue all of the credit and identification cards that have been lost
- Provides you with access to a robust database of contact information to quickly and easily get to the right person

Do I have to pay extra for this service?
Lost Wallet is included with your membership, and there are no extra fees.

Do you need my account numbers to cancel my cards?
No. Our Specialists will assist in contacting your bank or creditor to cancel your lost or stolen cards. These entities will be able to locate your account by verifying other forms of personal identifying information.

Should I notify customer support before traveling?
It's not necessary to contact us before traveling. If you are currently out of state, we will help in canceling your cards, and assist in contacting your state's DMV office to replace your identification. If you are traveling by air, we will provide additional steps for your flight. A police report may be needed as documentation for a lost or stolen wallet. If you are traveling outside of the United States, we will provide you the U.S. Embassy or Consulate office contact information for passport replacement.

I'm not sure what was in my wallet. Can you notify my banks and cancel all of my cards?
For your security, your bank or creditor will speak only with the account holder. We will assist in reviewing your account with you for any other cards that were possibly in your wallet, and contact those entities.

Identity Theft Insurance

Identity theft insurance provided under policies issued to ID Notify reimburses you for certain expenses in the event that your identity is compromised with a $1 million insurance policy.

Benefits:

- Insures you with a policy to protect financial losses in the event of identity theft
- Reimburses you for expenses related to identity theft restoration, including replacement of documents, traveling expenses, loss of income, child/elderly care, fraudulent withdrawals from a bank account and legal costs

Is there a deductible?
No – this is a $0 deductible service.

What expenses are covered?

Expenses related to restoring your identity, such as attorney fees and lost wages.

MARKETING BEST PRACTICES

Creating Need for an Identity Protection Product

Protecting your identity is not as cut and dry as it was before the digital age. Now, with advances in technology, identity thieves have many more tricks and tactics to collect sensitive information, especially in the online world. The prevalence of personal information available through social networking profiles and on the Internet in general have made it easier for cyber criminals to collect credentials and personal information. Using an identity theft protection service is the best way to minimize risk and protect your personal information from being misused. Doing this not only gives you added convenience and peace of mind, but also provides more advanced protection than you can achieve on your own. Identity theft can take many forms, from stealing your complete profile – all of your personal information – to gathering bits of your identity and combining that information with other data to create a synthetic profile, so it's also important to use a best-in-class identity theft protection product that monitors comprehensive credit and non-credit activity.

- **Credit:** There is no way to completely prevent identity theft, but the best way to minimize your risk is to protect your identity with an identity theft monitoring product or service.
- **Non-credit:** The best way to achieve comprehensive identity theft protection is to monitor both credit and non-credit loans.
- Early detection of fraud greatly reduces the financial, emotional and legal burden associated with identity theft
- People who use an identity theft monitoring product or service have more control over the safety of their family and their identity
- Support through the restoration process enables victims to quickly and easily get on with their lives

CSID Powered Messaging

1. CSID is the power behind a growing industry of identity protection solutions
2. CSID is the leading provider of global identity protection and fraud detection technologies for businesses, their employees, and consumers
3. With CSID's enterprise-level solutions, businesses can take a proactive approach to protecting the identities of their consumers all around the world
4. CSID's comprehensive identity protection products advance from credit monitoring to include a full suite of identity monitoring services; insurance and full-service restoration; and proactive breach mitigation and resolution

Industry-Specific Messaging

Financial

Help strengthen customer relationships and trust

- Financial institutions are the top vendor that consumers seek identity protection products from
- Trust is key when an industry specializes in managing people's money
- Security and protection become even more indispensable as more business is conducted online and financial transactions are completed online and through mobile devices

Unmatched authentication solutions

- When it comes to financial services and consumer money, security is critical
- We provide a variety of two-factor authentication solutions that go above and beyond basic passwords and knowledge-based-authentication security solutions
- We can also further secure the authentication process with knowledge-based authentication and PIN number distribution options

The financial industry is one of the most targeted when it comes to data theft; proactive identity protection and fraud detection mitigate the impact of these attacks quickly and easily

- Security attacks on financial institutions are expected to increase by nearly 30 percent over the next two years
- Our data protection and fraud detection services give financial institutions the ability to proactively protect consumer data, respond quickly in the event of a breach and mitigate liability by offering a prompt solution

Combat Consumer Financial Protection Bureau Regulations

- Inform consumers of any product offerings
- Use approved billing practices so that a consumer is only billed if they have authenticated and successfully enrolled in the product

Insurance

Extra security for an industry that sells peace-of-mind

- Online criminals often seek out insurance information to defraud and steal policyholders' identities
- The insurance industry relies on consumer trust – our identity protection and fraud detection solutions enhance trust and allow for an extra level of consumer security

Easy-to-implement solutions for a complex industry

- Our identity protection and fraud detection solutions offer a systematic approach to ensuring the security of personal information
- Our solutions are easy to implement, easy to scale for business needs and are able to transcend uniquely global differences in identity monitoring and financial systems

Gaming

The most comprehensive, proven solution for identity protection in the gaming industry

- We offer globally customizable identity theft protection and fraud detection solutions.
- Easy, reliable user experience is the same no matter the country or the language

A global solution for a very global industry

- We offer a powerful and robust identity protection product that is scalable globally and addresses regional language and identity requirements

A growing market faced with a growing threat

- As the online gaming market grows, so too does the threat of a data breach
- Most attacks happen in Asia, North America and Europe – which together comprise 70 percent of the global online game market

Government

Protecting identities for the public good

- It is the responsibility of every government agency and organization to maintain the public trust and faithfully serve constituents. Securing PII is vital to the trust of constituents and government employees
- As policies and data become increasingly accessible, the security of public information must be safeguarded. Our solutions will keep constituent and employee identities protected and help minimize the impact of data breaches, if they should occur

Solutions designed for all levels of government

- Government agencies are some of the most vulnerable - they have to do more with fewer resources and are often direct targets for data breach and theft
- Our identity protection and fraud detection solutions are completely scalable and customizable to work with each organization's level of risk, type of data housed and budget

Healthcare

A higher standard of technology for a higher standard of patient care

- We are the first identity protection and fraud detection solution provider to deliver a full-featured set of technologies that can be customized to the conditions of healthcare environments

Custom-fit services to address the continuum of care

- We offer a comprehensive collection of identity protection services that are completely customizable to fit the needs of all health service providers from small medical practices to regional hospitals
- Our Medical Identity Restoration product provides an added level of protection by providing patients with the safeguards they need in the event their medical identities are stolen

Telecommunications

Simple to implement, easy to scale, global in reach

- We provide an impressive array of identity protection and fraud detection services through a single, easy-to-access platform that can be customized to a user's needs, no matter where they are
- As consumers entrust more and more data to their service providers, we can lessen the impact if this data is stolen

Extra protection for a device that is central in day-to-day life

- Mobile phones aren't just for making calls anymore. They make financial transactions, store private information like passwords and business documents and company email and business contacts
- We provide users with a proactive approach to monitoring this data as well as a way to lessen the impact if this data is lost

Online/ecommerce

Identity protection and fraud detection is an industry where consumer PII is inherently at risk

- Online businesses operate in a wide range of industries. Regardless of their focus, protecting a consumer's PII and company information is essential

A global, scalable solution for an industry that has no borders

- An online store does have the same geographical limitations that a brick-and-mortar business is subject to
- We provide identity protection and fraud detection solutions that offer added security no matter where a customer may be or what they may be purchasing

Trust is paramount for repeat business

- Consumers have many options when shopping online – the added security that our products provide may be the difference that makes a repeat customer

Consumer

Consumers need to have a multi-layered approach to protecting their identities

- Additional safeguards are needed to protect one's identity as identity theft becomes more sophisticated and prevalent
- Multi-layered protection includes credit monitoring, CyberAgent, non-credit protection, restoration and identity theft insurance, amongst other services

Awareness is an effective weapon against most forms of identity theft

- Be aware of how information is stolen and what can be done to protect it
- Monitor personal information to uncover any problems quickly and know what to do in the event of a stolen identity

Small behavioral changes can help protect identity as well

- Monitor identity online and follow these simple tips:
    - Don't carry extra credit cards, your Social Security card, birth certificate or passport with you
    - Be careful when giving out personal information, and refuse to provide a Social Security number, as only a few organizations such as motor vehicle departments, tax departments and welfare departments have the right to ask for your number
    - Shred your records, credit card offers, bank statements, returned checks and any other sensitive information before throwing it away
    - Frequently check your credit reports and Public Record Profile to validate all of the information reported is correct
    - Use a locked mailbox to send and receive mail

Online Marketing Vehicles

Search Engine Optimization (SEO)

Search can be used to improve the visibility of a website, and improve the likelihood that it will show up in natural/un-paid search results. Search engines use sophisticated algorithms to index and find pages and present them in their search results, and these algorithms are constantly being updated and changed. There are a number of ways to boost SEO in-house, or if budget permits, an SEO specialist can be hired. To boost ranking in natural search for a website, consider these best practices:

- Perform a key word analysis to determine customers perceptions and interests as related to the website and business
- Define a list of key words that are relevant to the website and business
- Include key words in metadata, website content, links and URLs
- Optimize your website for mobile, as voice search is coming into play due to high mobile usage
- Utilize social media as an additional platform to interact with customers to drive traffic to your website

Search Engine Marketing (SEM)

Similarly to SEO, SEM uses search to drive customers to a website, but employs paid placements, links and display banners. To execute an SEM campaign, consider these best practices:

- Hire an agency or contractor specializing in SEM campaign strategies and execution
- Perform a key word analysis to determine customers perceptions and interests as related to the website and business
- Define a list of key words that are relevant to the website and business
- Include key words in metadata, website content and links
- Determine budget and campaign model (CPC vs. CPM)
- Leverage social media sites like Facebook have added Graph Search, targeted ads, marketing segmentation and contextual suggestions for users.
- Optimize for mobile, as more and more people will start accessing the Internet through their mobile devices

Social Media

Social media is a valuable marketing tool that can be used for customer acquisition, retention and research. Establishing company profiles on popular platforms like Facebook, LinkedIn and Twitter is a great way to connect and engage with customers in an environment that they are comfortable with. Use social media to communicate company news and promotions, understand customer motivation and get feedback on products. To use social media marketing effectively, consider these best practices:

- Define social media goals and metrics. What is the purpose of the effort and how will success be measured?
- Focus efforts. Find out where the customer is and go there (i.e. Facebook is the best place to engage with moms so maximize effort spent there to reach this group)
- Incorporate SEO and SEM key words in social media content
- Be mindful of post content. Don't use social media primarily as an advertising or promotional tool.
- Know your audience. Post content that is relevant to customers and promotes engagement with the brand
- Be mindful of post frequency. Don't overwhelm followers with too many posts, but keep the conversation fresh
- Be human. Create a personality and keep content aligned with that personality
- Be transparent. Encourage positive and negative feedback and respond to all of the above in a timely manner

Social Advertising

In conjunction with a social media presence on Facebook, Twitter and LinkedIn, social advertising can be used to increase a follower base, conduct research and raise awareness. The social networking communities' extensive member base and user knowledge allows businesses to reach a very specific customer with ads that let you target by age, location, interests and more. Costs can be customized to fit unique business needs, and campaigns can be continuously optimized. Companies may work with their social community of choice to set up an advertising strategy if more guidance/support is preferred, or can easily launch a campaign using the advertising dashboard without any assistance. To use social advertising effectively, consider these best practices:

- Define goal for campaign. What should the ad do and how will it be measured?
- Create budgets for your campaigns (CPC vs. CPM). This will help you decide which ads to run and when
- Research social advertising platforms. Familiarize yourself with your options so that you can make the best decision.
- Communicate a clear call to action and fit your social ad campaigns in the context of other advertising initiatives
- Match targeting options with advertising objectives
- Run multiple ads at once to gauge performance. Test different images, headlines and calls-to-action

Email Marketing

Email marketing is an effective tool for advertising company news and promotions, and for customer acquisition and retention. Emails can come in a number of forms from quarterly newsletters to product

promotions. To use email marketing effectively, consider the following best practices:

- Define goals for email program (what should customers do when they receive the email?)
- Include "opt-in" field on website homepage and in other relevant marketing materials
- Define editorial calendar and plan ahead
- Communicate regularly and on-schedule, but do not bombard customers with too many emails
- Include links to social media platforms
- Include "unsubscribe" link
- Ensure email campaign is CAN-SPAM compliant. This includes unsubscribe, content and sending behavior compliance
- Stay away from buying lists

Online Advertising

Online advertising is best used to drive customers to visit a website. Banners and rich media are the most commonly used creative pieces in this medium, and companies may work with a media or creative agency to purchase a media plan for said creative. Banners are simple creative executions that typically feature four to five frames of messaging with a call-to-action at the end. Rich media creative may include the use of video and audio clips, music and/or flash animation. They can be quite robust and interactive. These tools can be helpful in capturing audience attention and driving them to a website. To use online advertising effectively, consider the following best practices:

- Define goals for the campaign. What should the ad do?
- Select a media or creative agency to prepare a media plan. Creative and media placement will work together and will be defined during this stage in the process
- Communicate a clear call to action
- Define targeting
- Determine budget and campaign model (CPC vs. CPM)
- Run multiple ads at once to gage performance. Test different images, headlines and call-to-actions

Other Marketing Tactics

Testimonials

Using real testimonials can boost your credibility and provide a way for potential customers to relate to other identity theft protection users. These positive and believable testimonials serve as evidence to other customers that they should invest in the product. Consider these best practices when using testimonials:

- Include the name, city and even photos of the individuals providing the testimonial
- Be sure to ask permission before publicizing any personal information
- Use video testimonials when possible, but keep them short (30 seconds to one minute)

Blog

A blog offers an opportunity to express thought leadership and give (and gain) customer insight on a company, its products and the identity theft industry. It can also help to boost search rankings. By

posting relevant and interesting content to a blog, potential customers will be enticed to read and learn more. As a retention tool, blogs continue the conversation with customers, reminding them of the value of their identity protection service. Blog posts can include company/industry news, recent product launches, top 10 lists, or interesting identity theft statistics. When executing a blog, consider these best practices:

- Choose your blog platform; there is a wealth of information available on the web with tips on setting up a company blog through different platforms
- Keep blog posts at 450 words or less
- Use images and videos to attract readers and keep them interested

Example blog post:

'Tis the Season: Secure Your Business' Online Shop
November 14, 2013
Holiday season is just around the corner. Most people are aware that online holiday shopping opens up a number of security risks for consumers, and last year we outlined security tips for the online shopper during holiday seasons – but this year? Let's tackle the issue from the business side.

Businesses with online shops are surely looking forward to the season, especially Cyber Monday, the Monday after Thanksgiving, during which they'll likely see a huge boost in sales and popularity among their shoppers. But what about the security risks that comes with managing an online shop? Consider these tips to keep your business – and your shoppers – secure this holiday season.

- Keep your machines clean
- Train everyone in security and privacy basics
- Create user accounts for each customer
- Encourage strong passwords
- Protect sensitive customer information
- Secure your site and provide advice for shoppers

Click here to read the full article.

All of us at [Your Company's Name] wish you a safe, happy, and healthy Holiday Season!

Case Studies

Case studies can provide customers with relevant and notable examples of why identity protection products are important, and in doing so further solidify the need you're creating through marketing efforts. Consider these best practices when using case studies:

- Research common use-case scenarios and post case studies that are relevant
- Keep case studies simple and easy to digest
- Use case studies as fodder for social media posts, speaking engagements, byline articles and for other appropriate marketing opportunities

Example Identity Theft Cases:

Meet Mat Honan
Mat Honan, senior writer with Wired, had his entire digital life destroyed in the span of an hour by

hackers. Mat lost more than a year's worth of photos (covering the entire lifespan of his daughter), and important documents and emails. Mat's Google, Twitter and Apple ID accounts were linked, allowing the hacker to easily access all three.

Meet Naoki Hiroshima
Naoki experienced several breaches of online accounts including PayPal, GoDaddy and Facebook. The hacker responsible blackmailed Naoki into handing over control of his of Twitter handle, @N—a coveted one-character account that he was once offered $50,000 for.

Meet Olivia
Olivia is a child who participated in a 2012 survey sponsored by AllClear ID on the topic of child ID theft. When she went off to college, she applied for her first credit card to begin building her credit and financial independence. To her surprise, Olivia was denied and told that her SSN on her application did not belong to her. It was this event that first disclosed that an identity thief had been using her SSN since she was 9-years-old.

Meet Donald Bren
In 2010, Donald, one of Southern California's wealthiest men, made headlines when he fell victim to tax identity theft. A man who looked nothing like him walked in to an Orange County bank, opened accounts in Donald's name and deposited a $1.4-million federal tax refund check.

Meet Rene Bertagna
Last year, Rene closed his DC-area restaurant the Serbian Crown after nearly 40 years in the same location. Today, he is currently suing Google for the sudden drop-off in business that caused him to close his doors. Rene's Google Places listing was hijacked by a competitor that purported his restaurant was closed on the weekends, the time of the week that garnered the majority of his business. The 74-year-old Rene does not own a computer and was unaware when the misleading listing was posted.

Videos

Video offers a high quality, easy-to-digest experience to the customer during their information gathering process. When customers are researching and considering purchase of the product, videos can be an effective way to illustrate product value and can be easily shared between interested parties. A video caters to the population who prefer learning via watching and listening rather than reading through website content. When using video, consider these best practices:

- Incorporate SEO and SEM key words in video content and embed in relevant text pages on the website
- Keep videos short and sweet (2 minutes maximum in length)
- Consider working with a production company to ensure that the video quality is enterprise-level

Frequently Asked Questions (FAQ)

Incorporating an FAQ page on a website is a helpful way to address questions before customers contact sales or customer service. Questions and answers may range from how a product really works, to company and industry-focused. When using an FAQ, consider these best practices:

- Conduct information focus groups to determine what questions are truly most frequently asked

- Incorporate SEO and SEM key words into content
- Use the FAQs in this tool kit as guides

IDENTITY THEFT STATISTICS

Fraud in the United States

Key Messages

Javelin 2015 Identity Fraud Report:

- 12.7M: U.S. adult victims of identity fraud
- 5.2%: Fraud victims as a % of U.S. population
- $16B: Total annual fraud amount
- $1,228: Mean fraud amount per victim
- $293: Median fraud amount per victim
- $115: Mean consumer cost of fraud
- 8: Mean resolution time (hours)
- 2: Median resolution time (hours)

Federal Trade Commission Sentinel Network Data Book 2014:

- Over 1.5 million complaints were fraud-related. Consumers reported paying over $1.7 billion in those fraud complaints; the median amount paid was $489. 55% of the consumers who reported a fraud-related complaint also reported an amount paid.
- 46% of all fraud-related complaints reported the method of initial contact.
    - Of those complaints, 54% said the telephone, while another 23% said e-mail.
    - Only 4% of those consumers reported mail as the initial points of contact.

Supporting Messages

Javelin 2015 Identity Fraud Report:

- The number of victims of identity fraud decreased by 3% from 13.1 million in 2013 to 12.7 million in 2014. But the minor decline in incidence belies the fact that total fraud losses declined to $16 billion in 2014, a decrease of 11% from 2013 ($18 billion) – which can be attributed to improvements in the prevention and detection of fraud.
- Existing-account fraud (EAF) incidence saw a noticeable drop from 5% to 4.64%, but it still remained higher than the four years preceding 2013.
    - Losses due to EAF dropped 13% since last year to $14 billion.
- Despite a drop in existing-card fraud (ECF) incidence from 4.6% in 2013 to 4.42% in 2014, the number of debit or credit card fraud victims amount notified breach victims increased by 13%, claiming 7.2 million victims compared to 6.36 million in 2013.
- Account takeover (ATO) still affects relatively few consumers compared to other fraud types with an incidence of 0.63%, yet this is still the highest incidence this fraud type has seen in any year except 2013.
- New account fraud (NAF) reached record lows in 2014, yet these victims are 3 times more likely to take a year or more to discover that their identities were misused compared to other types of fraud.

Global Fraud

Ponemon Institute 2014 Cost of a Data Breach Study:

- Highest total cost of a breach / cost per record
  - US: $5.85M / $195
  - Germany: $4.74M / $201
- Lowest total cost of a breach / cost per record
  - Brazil: $1.61M / $70
  - India: $1.37M / $51
- Average number of breached records by country (top 3)
  - 29,087: US
  - 28,690: United Arab Emirates & Saudi Arabia
  - 26,586: India
- Main root cause of data breaches
  - 42%: Malicious or criminal attack
  - 30%: Human error
  - 29%: System glitch abnormal
- Countries with the highest churn rates following a data breach (top 3)
  - 4.5%: France
  - 4.0%: Italy
  - 3.4%: UK

Kroll Global Fraud Report, 2013/2014:

- 70% of companies reported suffering from at least one type of fraud in the past year, up from 61% in the previous poll.
- Percentage of companies affected by the following fraud types in 2013
  - 28%: Theft of physical assets
  - 22%: Information theft
  - 20%: Management conflict of interest
  - 19%: Vendor, supplier or procurement fraud
  - 16%: Internal financial fraud
  - 14%: Corruption and bribery
  - 11%: IP theft
  - 8%: Market collusion
  - 8%: Misappropriation of company funds
  - 3%: Money laundering
- More than two-thirds (68%) of companies plan to invest in IT security software next year to reduce exposure to information security incidents. And, 66% regularly conduct security assessments of their data and IT infrastructure.
- 72% of those surveyed say that their company has been hit by a fraud involving at least one insider in a leading role, slightly up from 67% last year.
- 30% report that entering new, riskier markets has increased their exposure to fraud in the past year. IN the same period, greater levels of outsourcing and offshoring raised fraud risk for 28% of those surveyed.
- Percentage of companies dissuaded from investing in (top 3):
  - 31%: Latin America
  - 27%: Central and Eastern Europe

- 25%: Africa
-

ID Theft

Federal Trade Commission Sentinel Network Data Book 2014:

- Government documents/benefits fraud (39%) was the most common form of reported identity theft, followed by credit card fraud (17%), phone or utilities fraud (13%), and bank fraud (8%).
  - Other significant categories of identity theft reported by victims were employment-related fraud (5%) and loan fraud (4%).
- 32% of identity theft complaints reported they contacted law enforcement.
  - Of those victims, 88% indicated a report was taken.
- Florida is the state with the highest per capita rate of reported identity theft complaints, followed by Washington and Oregon.

Child ID Theft

Key Messages

CSID 2012 Report, Child Identity Theft – A Parenting Blind Spot

- 87% of parents are involved in monitoring their child's online activity
- 56% of parents are aware that child identity theft is a growing trend
- 76% of parents are concerned that their child's identity might be stolen
- 52% of parents are not currently taking measure to prevent the misuse of their child's online information
- 88% of parents who are not currently taking measures to prevent the misuse of their child's information would be willing to do so
- 14% of parents who are currently taking preventative measures are using a monitoring service to watch for fraudulent activity

Javelin 2012 Child Identity Fraud Survey Report:

- One in 40 respondents had a child who was a victim of identity fraud (2.5%)
- 27% of victims reported knowing the individual responsible for the crime (friendly fraud), most likely a dependent's relative or family friend.
- A SSN is the top compromised identifier.
  - 56% of respondents reported theft or misuse of a child's SSN.
- Synthetic identities most common method of child id fraud.
  - When a child's SSN is combines with a different date of birth to create a fabricated identity used to commit fraud, which is extremely difficult to detect.
- Child Identity fraud takes and estimated 334 days to detect and 44 hours to resolve; 17% of children were victimized for a year or longer.
- As family income decreases, the risk of child identity fraud increases.

- 50% of households of child identity theft victims had incomes under $35,000, while only 10% of households of child identity theft victims had incomes of more than $100,000.

AllClear ID 2012 Child ID Theft Report

- The percentage of victims under the age of 5 more than doubled this year compared to last year- an increase of 105%
- Credit reports fail to detect 99% of child identity theft cases
- 10.7% of children had someone else using their Social Security numbers. This is an increase of .5% from the 10.2% rate reported in the 2011 report
- The rate of identity theft for children was 35 times higher than the rate for adults in the same population
- 15% of victims were five- years-old and younger, an increase of 105% over the 2011 findings and 26% of victims were six to ten-years-old, a 34% increase from the 2011 report
- One 19-year old victim had $1.5 million in fraud committed. Her Social Security number had been used fraudulently since she was nine-years-old
- In 2012, the number of suspects per child increased by 15% this year over the previous year's report

Supporting Messages

The FTC recommends all parents and guardians check their child's credit against the 3 credit bureaus when they turn 16, that way if there is a problem they have two years to get it fixed before they turn 18 and become an adult

Carnegie Mellon CyLab Child ID Theft Report

- Many commercial and public sector entities do not treat Social Security numbers as unique identifiers. It is possible for one SSN to appear on more than one credit file, employment report, criminal history – all mapped to different names
- One reason that minor SSNs are so valuable is that there is currently no process for organizations, like an employer or creditor; to check what name and birth date is officially attached to that SSN. As long as an identity thief has a SSN with a clean history, the thief can attach any name and date of birth to it
- In some cases, parents can open utility bills under their child's name and SSN to take advantage of the child's clean SSN. Most parents do not intend to harm their child's future, but in fact, this is identity theft
- When parents opt their children out of pre-approved credit card offers, it actually creates a credit file for the minor. These files cannot be deleted once created, but can be suppressed upon request of the parent. Parents need to contact each credit bureau regarding suppressing their child's file
- When parents try to deal with creditors to clean up issues, the creditors can ask to speak to the child – children as young as 1-2 years old – to verify their identity. Obviously creditors don't get very far using this method

- Children with the same name as a parent are frequently mixed up with their parents' credit file, causing them to have to deal with their same-name parents' credit – and any related issues. Mix-ups involving names can occur for different reasons.
    - Certain information is reported and does not contain a SSN (for example, civil judgments)
    - Collection agencies have been known to report debts only under name and address
    - While it is not a requirement for children to obtain SSNs, many hospitals include applying for an SSN as one of the steps for parents to complete before leaving the hospital with their newborn

Data Breaches

Key Messages

Javelin 2015 Identity Fraud Report:

- The number of debit or credit card fraud victims among notified breach victims increased by 13%, claiming 7.2 million victims compared to 6.36 million in 2013.
- 1 in 4 consumers received data breach notification in 2014, but a smaller proportion became fraud victims than in the previous year.
    - Fraud incidence among notified breach victims dropped to 13.7%, representing a 17 percentage-point drop since 2013. The massive number of data breach in 2014, combined with issuers replacing affected cards to appease consumer fear, could be key drivers of this decline.
- Data breaches had a great impact on consumer purchasing decisions with 28% of fraud victims would avoid dealing with certain merchants post-fraud.
    - This reaction is even more common among students who experienced identity fraud – 56% would avoid certain merchants – because fraud is more damaging to their current lifestyles.
- Credit cards are the most commonly breached, impacting more than half (51%) of data breach victims.
- Of the 61.2 million consumers notified of a data breach in 2014, nearly 8.5 million suffered fraud.

Verizon Data Breach Investigations Report, 2015:

- $400 million: The estimated financial loss from 700 million compromised records.
- Top three industries affected: Public, Information, and Financial Services.
- In 70% of the attacks where we know the motive for the attack, there's a secondary victim.
- In 60% of cases, attackers are able to compromise an organization within minutes.
- 75% of attacks spread from Victim 0 to Victim 1 within 1 day (24 hours). Over 40% hit the second organization in less than an hour.
- 23% of recipients now open phishing messages and 11% click on attachments.
    - Nearly 50% open email and click on phishing links within the first hour.
- 99.9% of the exploited vulnerabilities were compromised more than a year after the common vulnerabilities and exposures (CVE) was published.
- An average of 0.03% of smartphones per week – out of tens of millions of mobile devices on the Verizon network – were infected with "higher-grade" malicious code.

    - This is an even tinier fraction than the overall 0.68% infection rate (of all types of unwanted software).
- 95% of malware types showed up for less than a month, and four of five didn't last beyond a week.
    - 70-90% of malware samples are unique to an organization.
- In the 2014 DBIR, 92% of all 100,000+ incidents collected over the last 10 years fell into 9 basic patterns.
    - While there were many changes in the threat landscape in the last 12 months, these patterns still covered the vast majority of incidents (96%).
- Most affected industries
    - POS Intrusions: Accommodation, Entertainment, and Retail.
    - Payment Card Skimmers: Financial Services and Retail.
    - Crimeware: Public, Information, and Retail
    - Web App Attacks: Information, Financial Services, and Public
    - DOS Attacks: Public, Retail, and Financial Services
    - Physical Theft: Public, Healthcare, and Financial Services
    - Insider Misuse: Public, Healthcare, and Financial Services

Supporting Messages

Verizon Data Breach Investigations Report, 2014:

- 90% of breaches can be described by nine basic patterns: POS Intrusion, Web App Attacks, Insider Misuse, Physical Theft/Loss, Payment Card Skimmers, Crimeware, DoS Attacks, Cyber-Espionage, Miscellaneous Errors
- 99% of cases where methods were used to steam payment card information were detected by entities outside of the breached organization.
- Malware, including RAM scraper (85%) and Export data (79%) are the top threat action varieties within POS intrusions.
- Ideology/Fun is the primary motive within Web App Attacks (65%).
- Privilege abuse accounts for 88% of insider trading actions.
- 43% of physical theft and loss happens in the victims' work area.
- Misdelivery is the most frequently seen error resulting in data disclosure (44%).
- Credentials (82%), Bank (71%) and Payment (14%) are the top three at-risk data within Crimeware.
- ATMs are the most effected assets within Card Skimmers (87%).
- The United States is the greatest victim of Cyber Espionage (54%).
- The Financial industry is one of the top industries affected by Denial of Services Attacks.

Javelin 2014 Identity Fraud Survey Report:

- Nearly one in three data breach victims (30.5%) also suffered identity fraud in 2013 – up from 22.5% in 2012.
    - Among consumers who had their SSN breached, 16.1% suffered identity fraud in 2013 (compared with 27.7% in 2012).
    - Among consumers who had their debit card breached, 45.7% suffered identity fraud in 2013 (compared with 37.1% in 2012).
    - Among consumers who had their credit card breached, 35.1% suffered identity fraud in 2013 (compared with 24.3% in 2012).

    - Among consumers who had their credit card and/or debit card breached, 38.6% suffered identity fraud in 2013 (compared with 28.2% in 2012).
- Type of PII compromised in a data breach:
    - 41%: Credit card number
    - 21%: Debit card number
    - 14%: Social Security number
    - 14%: Other
    - 8%: Online banking log-in
    - 7%: Checking account number
    - 5%: Medical records or health insurance info
    - 5%: School or university records
    - 4%: ATM PIN on debit card
    - 3%: Credit card PIN
    - 2%: Driver's license number

Identity Fraud Lifecycle

Key Messages

Javelin 2015 Identity Fraud Report:

- Different fraud types directly correlate to their respective mean detection times.
    - Fraud is being detected within 37 days, which is 3 days slower than in 2013.
    - Fraudsters are still misusing consumers' information for an average of 47 days – that means it takes 10 days on average to stop the fraud from occurring after it has been detected.
- 33%: The percentage of victims that first discovered identity theft when notified by companies such as a bank or credit card provider.
- 2%: The percentage of victims that first discovered identity theft by using a credit monitoring or identity protection service.

Supporting Messages

Javelin 2015 Identity Fraud Report:

- Detection means:
    - 33%: Notified by companies such as a bank or credit card provider
    - 22%: By monitoring accounts through the Internet, ATM, or other electronic means
    - 11%: Notified by financial or fraud text alert
    - 11%: Found out some other way
    - 8%: By monitoring accounts through review of paper statements
    - 4%: When contacted by a debt collector or creditor
    - 3%: When turned down for credit
    - 3%: Notified by police, law enforcement, or other government agency
    - 2%: By review credit report
    - 2%: When reported lost or stolen cards or other documents to financial institution
    - 2%: Using a credit monitoring or identity protection service
- Detection time:
    - 99: Average number of days to detect new-account fraud
    - 52: Average number of days to detect account takeover

- 39: Average number of days to detect existing non-card fraud
- 38: Average number of days to detect existing non-card fraud (non-ATO)
- 37: Average number of days to detect all fraud

Cost of Fraud

Key Messages

Javelin 2015 Identity Fraud Report:

- Average Fraud Amount by Demographic
  - $1,288: All consumers
  - $1,245: Military
  - $1,246: Students
  - $822: Seniors
- Average Consumer Cost by Demographic
  - $155: All consumers
  - $107: Military
  - $135: Students
  - $7: Seniors

Ponemon Institute 2014 Cost of a Data Breach Study:

- The average cost of a data breach in the US is $5.85M per incident and $201 per record.
- The US moved into the #1 spot for greatest number of breached records at 29,087 records.
- The average cost post-data breach in the US is around $1.6M.
- The average lost business cost in the US is around $3.3M.

Password Management

Key Messages

Javelin 2014 Identity Theft Survey Report:

- Almost half of consumers use the same password to access multiple accounts.
  - If a consumers account is compromised, there is a 49% chance that it can be used to gain access on their other accounts
- Consumers with more than 20 accounts are nearly 50% more likely to experience fraud
- Around 50% of smartphone owners use a password or pattern, yet only 32% change a password or pattern periodically.

CSID 2012 Report, Password Habits: A Study of Password Habits Among American Consumers:

- 61% of consumers reuse the same password on multiple websites.
- 76% of 18-24 year-old consumers use the same password on multiple websites – more than any other age group.
- 54% of consumers have only five passwords or less.
- 44% of consumers change their password only once a year or less.
- 89% of consumers feel secure with their current password management and use habits.
- 21% of consumers have had an online account compromised.

Supporting Messages

Splashdata 2014 List of Most Popular Passwords

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football
11. 1234567
12. monkey
13. letmein
14. abc123
15. 111111
16. mustang
17. access
18. shadow
19. master
20. michael
21. superman
22. 696969
23. 123123
24. batman
25. trustno1

Consumer Profiles

Key Messages

Javelin 2015 Identity Fraud Report:

- Military personnel had the highest rate of NAF, similar to the rate of students. Military personnel suffered NAF at 28% higher rates (0.37%) than all consumers, causing the mean fraud about to rise to $1,245. Casual use of sensitive PII for everything from gym memberships to linking health records could be the primary driver for NAF.
- Despite the prevalence of card-related breaches, students are significantly less likely to experience card fraud than all consumers. Given that only half of students own a major credit card due to limitation inherent in the CARD Act of 2009, fraudsters have reduced opportunities for ECF. In turn, they shifted attention to more costly NAP, with a 45% higher incidence amount students compared to all other consumers.
- Security behaviors and fraud prevention practices are a huge concern among students and military personnel, leading to familiar fraud. Students may be adept at managing their cyberspace accounts, but they are lax about secure document storage and disposal habits.
    - Similarly, military personnel seem to use their common access cards (CACs) as a single identity reference document. Loss of such a card would lead to significant damage to

the individuals with perpetrators gaining access to sensitive PII such as full name and date of birth.
    - Such low-grade security standards lay the groundwork for familiar fraud, as students experienced this type of fraud at more than four times that of all consumers, while military personnel felt the pinch at an 18% higher rate than all consumers (0.26%).
- Seniors and military personnel are more likely to be notified of fraud through existing financial relationships or by monitoring their own accounts.
    - Yet, students are more likely to be notified only when they are turned down for credit or when they are contacted by a debt collector to settle the fraudulent accounts in their name. As a result, students take 30% longer on average to detect fraud compared to all fraud victims.

Supporting Messages

Federal Trade Commission Sentinel Network Data Book 2014:

- Fraud complaints by consumer age
    - 19 and under: 2%
    - 20-29: 14%
    - 30-39: 17%
    - 40-49: 18%
    - 50-59: 21%
    - 60-69: 18%
    - 70 and over: 10%

Javelin 2014 Identity Fraud Survey Report:

- Consumers earning $150K or more have the highest incidence of identity fraud
- 24% of individuals who earn $25K-$35 a year reported fraud had a “severe effect” on their lives.

INDUSTRY- SPECIFIC STATISTICS

Financial

Javelin 2015 Identity Fraud Report:

- Credit card and debit cards are among the most commonly breached credentials, together representing 83% of the information breached for all consumers.
- Financial institutions, such as a bank or credit card provider, remain the most common source to alert consumers to fraud with 33% of consumers detecting fraud via those companies.
- 11% of victims discovered fraud by financial or fraud text alerts

Identity Theft Resource Center, 2014:

- Banking/Credit/Financial sector breach statistics in 2014
    - 43 total breaches, representing 5.5% of all breaches
    - 1.2M records breached, representing 1.4% of all records breached
- The Banking/Credit/Financial industry has reported the least number of breaches for 9 of the past 10 years, with a 10-year average of 8.1%.

IBM 2014 Cyber Security Intelligence Index:

- Over 75% of incidents targeted 5 industries, with the Finance and Insurance industry representing 23.8% of security incidents.

Business

Identity Theft Resource Center, 2014:

- Business sector breach statistics in 2014
  - 258 total breaches, representing 33% of all breaches
  - 68.2M records breached, representing 79.7% of all records breached
- From 2007 to 2011, the Business sector, with a 10-year average of 34.3 percent, represented the largest percentage of breaches, often far surpassing the next highest category.

CSID: Small Business Security, June 2014:

- 43% of small businesses say their business credit score is important to the well being of their business, but only 26% even know their score.
- 41% of small business decision makers are concerned with the security threats and risks that come with human error.
- 32% of small businesses consider employee social media use to be a security risk for their business.
- 40% of small businesses work with third party vendors to help with security.
- 22% of small businesses plan to increase cybersecurity measures this year, up from 15% the year prior.

CSID: Risk Mitigation for Small Businesses, June 2013:

- 80% of small businesses store employee, customer and partner email addresses and phone numbers.
- 55% of small businesses store the Social Security numbers of employees, customers and partners.
- 58% of small business owners are most concerned about undetected malware as a security threat to their business.
- 24% of small business owners say the biggest obstacle to focusing on cyber security is the lack of budget to do so.
- 12% of small businesses have a breach preparedness plan in place.

Education

Identity Theft Resource Center, 2014:

- Education sector breach statistics in 2014
  - 57 total breaches, representing 7.3% of all breaches
  - 1.2M records breached, representing 1.5% of all records breached
- In 2005 and 2006, Education and Government/Military held the spots for most breaches, at 47.8% and 30.8% respectively.

Ponemon Institute 2014 Cost of a Data Breach Study:

- The Education industry has the second highest per capita data breach cost, averaging $294 per incident.
- 2.4%: Churn rate of Education industry (this is a relatively low churn rate compared to pharmaceutical, financial and healthcare organizations that average ~6% churn rate).

Privacy Rights Clearing House, 2014:

- Educational Institutions
  - 1,063,890: Number of records in database in 2014
    - 94% account for malware or hacking
  - 28: Number of breaches made public
    - 57% account for malware or hacking

Government

Identity Theft Resource Center, 2014:

- Government/Military sector breach statistics in 2014
  - 92 total breaches, representing 11.7% of all breaches
  - 6.6M records breached, representing 7.8% of all records breached
- In 2005 and 2006, Education and Government/Military held the spots for most breaches, at 47.8% and 30.8% respectively.

Privacy Rights Clearing House, 2014:

- Government and Military Institutions
  - 1,725,755: Number of records in database in 2014
    - 98% account for malware or hacking
  - 27: Number of breaches made public
    - 44% account for malware or hacking

Healthcare

Identity Theft Resource Center, 2014:

- Medical/Healthcare sector breach statistics in 2014
  - 333 total breaches, representing 42.5% of all breaches
  - 8.3M records breached, representing 9.7% of all records breached
- The Medical/Healthcare sector, with a 10-year average of 26.4%, took over the top spot in 2012 on, attributing primarily to the mandatory reporting requirement for healthcare breaches being reported to the Department of Health and Human Services (HHS).
  - In 2005, this category reported the least number of breaches.

CSID: Finding a Cure for Medical Identity Theft, October 2014:

- 85% of healthcare organizations feel their systems adequately limit the risk of breach
- 17% of healthcare organizations are worried or very worried about losing patient data in a breach
- 41% of healthcare organizations spend 10% or less of their IT budget on protecting patient data against breach
- 50% of healthcare employees who have access to patient EHRs also have access to their personal email at work
- 32% of healthcare organizations use multi-factor authentication to access sensitive information

Ponemon Institute 2014 Study on Medical Identity Theft:

- 2.32M: The number of medical identity theft victims in the U.S. in 2014.

- 65% of medical identity theft victims in the study had to pay an average of $13,500 to resolve the crime.
    - In some cases, they paid the healthcare provider, repaid the insurer for services obtained by the thief, or they engaged an identity service provider or legal counsel to help resolve the incident and prevent future fraud.
- On average, victims learned about the theft of their credentials more than 3 months following the crime and 30% do not know when they became a victim.
    - Of those respondents (54%) who found an error in their Explanation of Benefits (EOB), about half did not know whom to report the claim to.
- Only 10% of respondents report achieving a completely satisfactory conclusion of the incident.
    - Those who resolved the crime spent, on average, more than 200 hours on such activities as working with their insurer or healthcare provider to make sure their personal medical credentials are secured and can no longer be used by an imposter and verifying their personal health information, medical invoices and claims and electronic health records are accurate.
- 45% of respondents say medical identity theft affected their reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions (89% of respondents).
    - 3% say it resulted in loss of employment.
- 79% of respondents say it is important for healthcare providers to ensure the privacy of their health records.
    - 48% say they would consider changing healthcare providers if their medical records were lost or stolen.
    - If such a breach occurred, 40% say prompt notification by the organization responsible for safeguarding this information is important.
- 25% of victims knowingly permitted a family member or friend to use their personal identification to obtain medical services and products; and 24% say a member of the family took their credentials without their consent.

Telecommunications

Javelin 2015 Identity Fraud Report:

- Two of the most difficult types of account takeovers to resolve – utility and mobile account attacks – saw dramatic improvements in detection and misuse times.
    - Additionally, utilities/mobile phone account takeovers declined dramatically to 15% from their high of 29% in 2013.
- Almost half (41%) of consumers receive email or mobile alerts about their credit card or checking account.

Javelin 2015 Push Notification Change the Game for Financial Alerts:

- Financial alerts will reach over half of the online U.S. population by 2019. Javelin forecasts that alerts will reach a milestone within five years: 52% of consumers will receive an email, SMS text, or push notification alert from their primary financial institution during a 12-month period.
- About 43% of consumers have received notifications in the previous 90 days from one or more of the apps they have downloaded. Only 13% of consumers received notification from their banking apps – putting FIs in the pack behind apps for social networks, “utility” apps like calendars, and instant messaging.

Verizon 2015 Data Breach Investigations Report:

- An average of 0.03% of smartphones per week – out of tens of millions of mobile devices on the Verizon network – were infected with "higher-grade" malicious code.
    - This is an even tinier fraction than the overall 0.68% infection rate (of all types of unwanted software) from Kindsight Security Labs' biannual report.
- Android: 96% of mobile malware was targeted at the Android platform.
    - More than 5 billion downloaded Android apps are vulnerable to remote attacks.

Online/e-Commerce

Javelin 2015 Identity Fraud Report:

- 28% of fraud victims would avoid dealing with certain merchants post-fraud. This reaction is even more common among students who experience identity fraud – 56% would avoid certain merchants – because fraud is more damaging to their current lifestyles.
- 19% of fraud victims spend less money online post-fraud. This reaction is even more common among seniors (19%) and Military (22%).
- Large retail chains take a hit as fraud victims avoid these merchants at more than twice the rate of 2013. Fraud victims avoided the following merchants post fraud:
    - 37%: Smaller online merchants
    - 24%: Online gaming or gambling websites
    - 22%: Large retail chain stores (such as Macy's, Target, Wal-Mart)
    - 21%: Small regional or local retail stores
    - 20%: Other
    - 15%: Larger online merchants (such as Amazon, eBay, and Zappos)
    - 12%: Restaurants, cafes, and coffee shops
    - 8%: Grocery stores, pharmacies, or other general merchants

FREQUENTLY ASKED QUESTIONS

General Questions

What is identity theft protection service enrollment process like?
You will first be asked to provide some information that authenticates your identity. We offer authentication options for high-risk transactions, which provide an additional layer of protection for individual identities and implement highly secure access to your profile. Some of our authentication solutions also enable you to reliably verify your identity via a mobile device.

How do you keep my information safe?
We maintain a highly secure environment with specific security measures and policies in place to ensure the utmost secure handling of all data.

How should I dispose of old records?
Old personal records should be shredded before being thrown away. If personal files are thrown out without being shredded, an identity thief could steal them from the trash. If your records are stored, is it with a secure document facility? Many businesses use a pick-up shredding service to dispose of old documents. Ask how long your records will be kept before they are deleted or destroyed. Companies know that privacy concerns are important to their customers. Data theft is common at universities, medical offices, financial institutions, and other businesses that keep records about you. A trustworthy

company should be able to quickly and honestly answer all five of your privacy questions.

How do I know if a company has had a security breach?
In many states, businesses must announce when they have experienced a theft or loss of personal data. Ask companies if they have ever had records stolen, if anyone has hacked into their computer system, or if they have ever lost sensitive data. Search online to see if there have been any security problems in the company's past.

What is the Fair Credit Reporting Act?
The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FCRA gives consumers specific rights (summarized below). You may have additional rights under state law.

You must be told if information in your file has been used against you. Anyone who uses information from a consumer reporting agency to deny your application for credit, insurance or employment or take another adverse action against you must tell you, and give you the name, address, and phone number of the agency that provided the information.

You can find out what is in your file. At any time, you may request and obtain your report from a consumer-reporting agency. You are entitled to free reports if a person has taken adverse action against you because of information in a report; if you are the victim of identity theft or fraud; if you are on public assistance; or if you are unemployed but expect to apply for employment within 60 days. In addition, you are entitled to one free report every 12 months from each of the nationwide credit reporting agencies and from some specialized consumer reporting agencies.

You have a right to know your credit score. For a fee, you may request your credit score. In some mortgage transactions, you will receive credit score information without charge.

You can dispute inaccurate information with the consumer-reporting agency. If you tell a consumer-reporting agency that your file has inaccurate information, the agency must take certain steps to investigate unless your dispute is frivolous.

Inaccurate information must be corrected or deleted. A consumer-reporting agency or furnisher must remove or correct information verified as inaccurate, usually within 30 days after you dispute it. However, a consumer-reporting agency may continue to report negative data that it verifies as being accurate.

Outdated negative information may not be reported. In most cases, a consumer-reporting agency may not report negative information that is more than 7 years old, or bankruptcies that are more than 10 years old.

Access to your file is limited. A consumer reporting agency may provide information about you only to people with a valid need as determined by the FCRA - usually to consider an application with a creditor, insurer, employer, landlord or other business.

Identity theft victims and active-duty military personnel have additional rights. Victims of identity theft have new rights under the FCRA. Active-duty military personnel who are away from their regular duty station may file "active duty" alerts to help prevent identity theft.

For more information, go to www.ftc.gov/credit, or write to: Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580

What is the Federal Trade Commission?
The Federal Trade Commission (FTC) enforces a variety of federal antitrust and consumer protection laws, including the federal Fair Credit Reporting Act, the law that regulates consumer-reporting agencies, those who use credit reports, and those who furnish information to consumer reporting agencies. The FTC ensures that all three parties (consumers, consumer reporting agencies, and lenders) are treated in a fair and equitable manner.

The FTC's mission is to help the nation's markets function competitively and efficiently, unhampered by needless restrictions. It works to spotlight and eliminate acts or practices that are unfair or deceptive. In general, the FTC tries to stop actions that threaten consumers' opportunities to exercise informed choice. It also performs economic analyses, when asked, to support its law enforcement efforts and to contribute to the policy as set forth by Congress, the Executive Branch, other independent agencies, and state and local governments.

In addition to carrying out its statutory enforcement responsibilities, the FTC advances the policies underlying Congressional mandates through cost-effective non-enforcement activities, such as consumer education.

Identity Theft Questions

What is identity theft?
You may have heard of identity theft, but what does this term really mean? Going far beyond credit card fraud, identity theft is a rapidly growing crime that most people will face at some point in their lives. Identity theft is officially defined as the deliberate assumption of another person's identity. It is a crime where a criminal acquires and uses the victim's personal information, such as a Social Security or driver's license number, to take out loans, obtain new credit cards, rent an apartment, purchase a car, run up debt, file for bankruptcy and other criminal activities. Identity theft can not only damage someone's creditworthiness, it can also create unknown criminal records that can result in the identity theft victim being wrongly arrested or denied employment after a routine background check.

How is identity theft different from financial fraud?
The term "financial fraud" covers common credit card, check, and debit card fraud. When a criminal uses your credit cards or debit cards to make a purchase, he or she usually hasn't assumed your identity. Recovering from financial fraud is usually easy, since most creditors don't hold you liable for fraudulent charges. These days, financial fraud is increasingly grouped into the same category as serious identity theft. The FTC combined both types in a report announcing that there were 9.9 million cases of identity theft in 2003. These crimes alone cost businesses $27.6 billion and cost consumers $5 billion directly in losses every year.

How does the identity thief get my information?
Identity thieves use a variety of methods to gain access to your personal information:

- Steal records from their employer, bribe an employee who has access to the records, con information out of employees, or hack into the organization's computers
- “Dumpster dive" through your trash at home or work to find bills and credit statements that

contain personal information
- Fraudulently obtain credit reports by either posing as a perspective landlord or misusing an employer's authorized access to credit reports
- Steal credit and debit card account numbers by using a special information storage device in a practice known as "skimming"
- Steal wallets and purses containing identification and credit and bank cards
- Steal your mail or complete a change of address to redirect your mail so that they will receive your credit card statements or tax information
- Use camera phones to take a picture of your credit or personal information while you complete a retail transaction
- Steal personal information from your home
- Scam information from you by posing as a legitimate business person or government official

What can I do to protect myself from identity theft?
Identity theft is a serious problem affecting more people every day. That's why learning how to prevent it is so important. Knowing how to prevent identity theft makes your identity more secure. The more people who know how to prevent identity theft, the less inclined others may be to commit the crime.

Preventing identity theft starts with managing your personal information carefully and sensibly. We recommend a few simple precautions to keep your personal information safe:

Only carry essential documents with you. Not carrying extra credit cards, your Social Security card, birth certificate or passport with you outside the house can help you prevent identity theft.

Keep new checks out of the mail. When ordering new checks, you can prevent identity theft by picking them up at the bank instead of having them sent to your home. This makes it harder for your checks to be stolen, altered and cashed by identity thieves.

Be careful when giving out personal information over the phone. Identity thieves may call, posing as banks or government agencies. To prevent identity theft, do not give out personal information over the phone unless you initiated the call.

Your trash is their treasure. To prevent identity theft, shred your receipts, credit card offers, bank statements, returned checks and any other sensitive information before throwing it away.

Make sure others are keeping you safe. Ensure that your employer, landlord and anyone else with access to your personal data keeps your records safe.

Stay on top of your credit. Make sure your credit reports are accurate and that you sign up for a credit monitoring service, which can alert you by email to changes in your credit report – a helpful way to prevent identity theft.

Protect your Social Security number. To prevent identity theft, make sure your bank does not print your SSN on your personal checks.

Follow your credit card billing cycles closely. Identity thieves can start by changing your billing address. Making sure you receive your credit card bill every month is an easy way to prevent identity theft.

Keep a list of account numbers, expiration dates and telephone numbers filed away. If you wallet is stolen, being able to quickly alert your creditors is essential to prevent identity theft.

Create passwords or PIN numbers out of a random mix of letters and numbers. Doing so makes it harder for identity thieves to discover these codes, and makes it easier for you to prevent identity theft.

How can I tell if I am a victim of identity theft?
Consistently monitor both your financial and public record information and look for:

- Unfamiliar criminal records, court records, address information or bankruptcies
- Unexplained charges or withdrawals
- Failing to receive bills or other mail. This may signal an address change by the identity thief
- Being served court papers or arrest warrants for actions you did not commit
- Receiving credit cards for which you did not apply
- Being denied credit for no apparent reason
- Receiving calls or letters from debt collectors or businesses about merchandise or services you did not buy

Although any of these indications could be a result of a simple clerical error, you should not assume that there's been a mistake and do nothing. Always follow up with the business or institution to find out

What should I do if I am a victim of identity theft?
Please contact our Restoration Specialists for help at 1-XXX-XXX-XXXX. In addition, according to the U.S. Attorney General's office, the Secret Service oversees identity theft. This office advises you to:

- Report the crime to the police immediately. Get a copy of your police report or case number. Credit card companies, your bank, and the insurance company may ask you to reference the report to verify the crime
- Immediately contact your credit card issuers. Get replacement cards with new account numbers and ask that the old account be processed as "account closed at consumer's request" for credit record purposes. You should also follow up this telephone conversation with a letter to the credit card company that summarizes your request in writing
- Call the fraud units of the three credit reporting bureaus and ask that your accounts be flagged. Also, add a victim's statement to your report that requests that they contact you to verify future credit applications:

  Equifax Credit Information Services - Consumer Fraud Div. P.O. Box 105069, Atlanta, Georgia 30348 Tel: (888) 766-0008, www.equifax.com

  TransUnion Fraud Victim Assistance Center P.O. Box 6790, Fullerton, CA 92834 Tel: (800) 680-7289, www.transunion.com

- Keep a log of all conversations with authorities and financial entities. And follow-up! Make sure that all creditors or credit bureaus have received what they need from you
- Review your reports regularly and make sure all changes you requested have been effected

Credit Questions

Credit Monitoring

What is Credit Monitoring?
Credit Monitoring includes monitoring of changes reported to one or all three national credit bureaus (Experian, Equifax and TransUnion) depending on whether you have single or tri-bureau monitoring enables. Changes monitored include personal information, public records, inquiries, new account openings, and existing accounts reported past due.

What should I do if I receive an alert for something that didn't happen?
In some cases, the credit-reporting agency may commit errors on your credit file and the incorrect information may trigger an alert. Nevertheless, if you see a credit alert that is not accurate; please contact a [[global_system-company_name]] Specialist at [[global_system-support_phone]] or by email at [[global_system-support_email]].

How often is my credit monitored?
Credit bureau alerts are generated through consistent monitoring, and are distributed multiple times a day. A credit bureau file is monitored daily and any alerts triggered as a result of new inquiries and/or adjustments made to a credit file are sent to you via email.

Credit Reports

What should I do if I see a mistake on my credit report?
In some cases, the credit-reporting agency may commit errors on your report - the incorrect information may simply be a mistake. However, an error on your credit report could indicate that an identity theft event has occurred. If you see incorrect information on your credit report, please contact a [[global_system-company_name]] Specialist at [[global_system-support_phone]] or [[global_system-support_email]].

Why is there a difference between my three scores?
Each credit-reporting agency generates a score derived from what is reported about you. A creditor may report to one, two or all three of the national credit bureaus. As a result, the information one credit bureau has may be different than another, resulting in a different credit score.

What time range does my initial credit report cover?
Your credit report includes data beginning from the date your credit file was first established. This could span more than 25 years.

Score Plotter

What does it mean if I see big changes in my credit score from month to month?
Every reported item on your credit report is used to calculate your credit score. If your score has changed significantly since the last month, it may be due to the fact that an account was not reported for the month or an item has been added to or removed from your report. Drastic changes in account balances and opening new lines of credit could also significantly impact your score.

How many months does Score Plotter show me?

Score Plotter tracks your credit score for past 12 months.

Is the credit score that Score Plotter plots related to a specific bureau?
Yes. Score Plotter tracks your TransUnion credit score.

Comprehensive Identity Questions

CyberAgent®

What information do I enter in the Medical Identities field?
Enter your Member ID number as it appears on your health insurance card.

Where does [[service_cyberagent]]'s data come from?
[[service_cyberagent]]'s data comes from Internet forums and websites, web pages, IRC channels, refined PII search engine queries, Twitter feeds, P2P sources, hidden and anonymous web services, malware samples, botnets, and torrent sources.

What time range does my initial [[service_cyberagent]] report cover?
Your first [[service_cyberagent]] report includes data from the previous 8 years. This means that [[service_cyberagent]] searches the prior 8 years of records it has collected for a match to the personal information you are monitoring.

What does it mean when I receive an alert?
Your [[service_cyberagent]] service tracks Internet activity for signs that the personal information you've asked us to monitor is being traded and/or sold online. This alert means that our surveillance technology has discovered information on the Internet that is a match to your monitored identity elements.

What if the alert references only some of the personal information [[service_cyberagent]] is tracking?
Even if only some of your personal information that has been detected by [[service_cyberagent]], it is recommended that you contact the appropriate institution to have your account information changed, or change your account information yourself if possible - like it would be with the password to your email account. It is safe to assume that if some of your information is compromised, all of it is. You may also want to review a copy of your credit report to ensure that all of the information that appears there is familiar to you.

Is the buying and selling of others' personal information online illegal?
This activity is illegal in the United States, but other countries do not necessarily have the same laws as related to cyber crime. United States regulatory agencies have no jurisdiction to prosecute fraudsters acting on websites and chat rooms located in other countries.

Can I still become a victim of identity theft even though I am enrolled in [[service_cyberagent]]?
[[service_cyberagent]] dramatically reduces your risk of identity theft by letting you know sooner if your personal information is compromised, and in turn enabling prevention or quick resolution of an identity theft incident. In addition to [[service_cyberagent]], you also have identity protection insurance and recovery services to help alleviate some of the financial burden of identity theft and guide you through the often confusing and difficult process. Unfortunately, no identity protection tool can prevent identity theft altogether.

Social Security Number Trace

What do I do if there is a name or address in the SSN Trace report that I don't recognize?
If your report contains names and/or addresses that are not familiar to you, there is probably an error in public records information. However, this could be an indication of identity theft. If you see unfamiliar information in your SSN Trace report, please contact a [[global_system-company_name]] Specialist at [[global_system-support_phone]] or [[global_system-support_email]].

What do I do if an old address is incorrect in the SSN Trace report?
It is not uncommon for address history dating back more than 5 years to contain errors. However, if the incorrect address is more recent, please contact a [[global_system-company_name]] Specialist at [[global_system-support_phone]] or [[global_system-support_email]].

What do I do if I see a name on the SSN Trace report or alert that isn't my current name?
It's not uncommon to see alternate names on your report due to marriage, joint credit accounts and nicknames you may have used. However, if you are concerned, please contact a [[global_system-company_name]] Specialist at [[global_system-support_phone]] or [[global_system-support_email]].

What time range does my initial SSN Trace report cover?
Your first SSN Trace report looks at data beginning from the date your SSN first entered public records. This could be as early as when you were born and issued an SSN.

Court Records Monitoring

Why doesn't my Court Records report have any information in it?
This is usually a good thing! It means that we didn't find a match to your personal information in our court records data. This may be due to one of the following:

- You have never been convicted of a crime
- Your identity has not been stolen for the purpose of committing a crime
- Your court records have been expunged or your court records have not yet been updated in the public records database

What records does Court Records Monitoring search for my personal information?
Court Records Monitoring searches court records and bookings data sourced from the following places:

- Over 509 million criminal court records mapping to federal, state, city, and county level jurisdictions
- Over 60 million incarceration records spread across 2,100 police organizations covering over 70% of national bookings
- 99 million Department of Corrections (DOC) parole, probation, and incarceration records
- Over 4.9 million warrant records. 98 county, state and city level warrants reporting 664 of 3,248 counties in 50 states and Puerto Rico
- Over 9 million arrest records
- Over 330 thousand government records, such as Most Wanted and terrorist lists

Does Court Records Monitoring report on records from all states and counties?
No. Court records data restricted states and territories include Maine, Wyoming, South Dakota, District of Columbia, and Puerto Rico. Department of Corrections data restricted states include Arkansas,

Colorado, District of Columbia, Delaware, Hawaii, Massachusetts, South Dakota, Virginia, Washington and Wyoming. Bookings data restricted states and territories include Arkansas, District of Columbia, Delaware, Hawaii, Kansas, Massachusetts, Maine, Montana, North Dakota, Nebraska, New Hampshire, Pennsylvania, Puerto Rico, South Dakota, Vermont, Washington, and Puerto Rico.

What if I see court records in the report that aren't mine?
False matches in court records report can occur as a result of an individual having the same name and/or date of birth as you. This can usually be resolved by calling the relevant courthouse to make sure the records belong to another individual. If the courthouse confirms that the records in question relate to your identity – usually done by confirming your SSN or driver's license number – and you did not commit the infraction, you may be a victim of identity theft. If you are concerned, please contact a [[global_system-company_name]] Specialist at [[global_system-support_phone]] or [[global_system-support_email]].

How soon will I receive an alert after a new court record is entered or a booking incident occurs?
You should see an alert within a month from the date a new court record is entered, and within 48 hours from the time a booking incident occurred.

What time range does my initial Court Records Monitoring report cover?
Your first Court Records Monitoring report includes court and bookings data from the past 10 years.

Non-Credit Loan Monitoring

What is a non-credit loan?
Non-credit loans include both payday and quick-cash loans that do not require a SSN or credit inquiry to complete. Non-Credit Loan Monitoring alerts users if this type of loan has been opened using an element of their identity.

How many non-credit loan establishments does Non-Credit Loan Monitoring report cover?
Non-Credit Loan Monitoring gets data from 23 of the top 25 payday lenders.

What time range does my initial Non-Credit Loan Monitoring report cover?
Your first Non-Credit Loan Monitoring report includes data from the past 2 years.

Sex Offender Monitoring

What records does Sex Offender Monitoring search for my personal information?
Sex Offender records are generated from entries in the national Sex Offender Registry (SOR). Sex Offender Monitoring searches a database of over 1.8 million records from 49 state registries as well as Washington DC, Native American reservations, Guam, Puerto Rico, and the US Virgin Islands. Mississippi does not allow access to its records, but information about Sex Offenders in this state are still included in our database when offenders have moved there from other states.

Are all Sex Offenders required to register in the national Sex Offender Registry (SOR)?
Not all criminals convicted of a sex-related offense are required to register with the SOR. The SOR includes only those offenders who were ordered to register via a criminal court case in their jurisdiction. Sex Offenders who were not ordered to register with the SOR would still appear in a criminal records database, and could have an offense description indicating a sex crime.

What if I see my name used by an offender in the Sex Offender Monitoring report?
False matches in this report can occur as a result of an individual having the same name and/or date of birth as you. This may also indicate that a Sex Offender has used your name or personal information to register.

A false match can usually be resolved by calling the relevant courthouse to make sure the records in question belong to another individual. If the courthouse confirms that the records in question relate to your identity – usually done by confirming your SSN or driver's license number – and you have not been convicted of a sex crime, you may be a victim of identity theft. If you are concerned, please contact a [[global_system-company_name]] Specialist at [[global_system-support_phone]] or [[global_system-support_email]].

How often is my Sex Offender Monitoring report updated?
Your Sex Offender Monitoring report is updated monthly. If there is a change in the data returned at this time, you will receive an alert.

Change of Address Monitoring

Where does Change of Address Monitoring data come from?
Change of Address Monitoring reports only changes in address that have been processed through the United States Postal Service (USPS). Change of Address Monitoring does not track UPS or FedEx-only addresses or private mailboxes.

How long after I submit a change of address request will I receive an alert?
The USPS can take up to two weeks after the "effective date" to publish the address change. CSID will alert you once the change has been published.

What do I do if there is an address in the Change of Address Monitoring report that I don't recognize?
If your report contains an address that is not familiar to you, there is probably an error in public records information. However, this could be an indication of identity theft. If you see unfamiliar information in your Change of Address Monitoring report, please contact a [[global_system-company_name]] Specialist at [[global_system-support_phone]] or [[global_system-support_email]].

What time range does my initial Change of Address Monitoring report cover?
Your first Change of Address Monitoring report includes data from the past 3 months, including the current month.

Self-Service Restoration

If I am experiencing more than one type fraud due to identity theft, how do I receive the necessary steps to restore all of my issues?
If your identity theft situation spans more than one type of fraud, simply take the restoration questionnaire focusing on one item needing dispute. Once you have reached the end of the questionnaire and the restoration guide is presented for the first issue type, download or print the restoration guide for future reference. When you have successfully downloaded or printed the first restoration guide, start the questionnaire over. This time, focus on the second identity theft issue type

that needs to be disputed until you have reached the second restoration guide. Repeat this process until you have the restoration guides to restore all of your identity theft issue types.

What are dispute templates used for and how do I download them?
A dispute template is a downloadable word document that provides you a pre-formatted notice to report identity theft and dispute the fraudulent item with the affected entity. Each dispute template is tailored to the specific type of identity theft occurring to ensure your disputes are handled appropriately. Links to download the dispute templates are provided in the steps of your restoration guide.

How do I print or download a copy of my restoration guide?
Once you've reached your restoration guide, you can print or download the full copy by selecting the print or download buttons located at the bottom right corner below the final steps of the restoration guide. Selecting the print or download buttons will provide all the information within your restoration guide so there is no need to expand each of the steps before selecting an option.

I took the questionnaire and it advised that I do not appear to be a victim of identity theft. How can I be sure?
Use your best judgment based on the information provided to you by the affected entity. If you still feel you are a victim of identity theft after taking the questionnaire, please contact the assisted restoration team to further research your incident by contacting [[global_system-support_phone]].

Insurance

Is there a deductible?
No – this is a $0 deductible service.

What expenses are covered?
Any expense related to restoring your identity, such as attorney fees and lost wages.

Lost Wallet

Do I have to pay extra for this service?
Lost Wallet is included with your membership, and there are no extra fees.

Do you need my account numbers to cancel my cards?
No. Our Specialists will assist in contacting your bank or creditor to cancel your lost or stolen cards. These entities will be able to locate your account by verifying other forms of personal identifying information.

Should I notify [[global_system-company_name]] before traveling?
It's not necessary to contact us before traveling. If you are currently out of state, we will help in canceling your cards, and assist in contacting your state's DMV office to replace your identification. If you are traveling by air, we will provide additional steps for your flight. A police report may be needed as documentation for a lost or stolen wallet. If you are traveling outside of the United States, we will provide you the U.S. Embassy or Consulate office contact information for passport replacement.

I'm not sure what was in my wallet. Can you notify my banks and cancel all of my cards?

For your security, your bank or creditor will speak only with the account holder. We will assist in reviewing your [[global_system-company_name]] account with you for any other cards that were possibly in your wallet, and contact those entities.