Identity & Credit Monitoring

SPOTLIGHT ID

Things You Should Know

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.

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 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 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 things 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 855-443-3684 (1-855-4-IDENTITY). In addition to starting a case with a Restoration Specalist, according to the U.S. Attorney General's 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:

- Experian Fraud Division - 1 888 397 3742
- Equifax Fraud Division - 1 800 525 6285
- TransUnion Fraud Division - 1 800 680 7289

- 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.

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.

Overview & Product Descriptions

What is the 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.

About: ID Agent Cyber Monitoring

What Identity Elements do you Monitor?

- Credit /Debit Cards
- Bank Account/Routing Numbers
- Full 9-Digit SSN
- Email Addresses
- Medical ID Numbers
- Driver's License Numbers
- Phone Numbers
- Passport Numbers
- IBANs
- Retail Cards

What information do I enter in the Medical Identities field?

Enter your Member ID number as it appears on your health insurance card.

What is bank Account Takeover Monitoring and Credit Card Application Monitoring?

Notifies you if your personal information has been used to apply for or open a credit card account; apply for or open a bank account; or if changes have been made to your existing bank account, including changes to the account holder's personal information or attempts to add new account holders.

Where does ID Agent's Cyber Monitoring data come from?

ID Agent's Cyber Monitoring 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 ID Agent Cyber Monitoring report cover?

Your first ID Agent Cyber Monitoring report includes data from the previous 8 years. This means that ID Agent Cyber Monitoring 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 ID Agent Cyber Monitoring 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 ID Agent Cyber Monitoring is tracking?

Even if only some of your personal information that has been detected by ID Agent Cyber Monitoring, 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 your credit report to ensure that all of the information 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 cybercrime. 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 Monitoring?

ID Agent Cyber Monitoring 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 ID Agent Cyber Monitoring, 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.

About: 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 Restoration Specialist at 855-443-3684 (1-855-4-IDENTITY).

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.

About: 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 Restoration Specialist at 855-443-3684 (1-855-4-IDENTITY).

Why is there a difference between my 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.

About: Credit 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 the past 12 months.

Is the credit score that Score Plotter plots related to a specific bureau?

Yes. Score Plotter tracks your Experian credit score.

About: 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 an ID Agent Specialist at 844-ID AGENT or support@IDAgent.com.

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, contact a Restoration Specialist at 855-443-3684 (1-855-4-IDENTITY).

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 Restoration Specialist at 855-443-3684 (1-855-4-IDENTITY).

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.

About: 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:

- More than 509 million criminal court records mapping to federal, state, city, and county level jurisdictions
- More than 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
- More than 4.9 million warrant records. 98 county, state and city level warrants reporting 664 of 3,248 counties in 50 states and Puerto Rico
- More than 9 million arrest records
- More than 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 Restoration Specialist at 855-443-3684 (1-855-4-IDENTITY).

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.

About: Court Records 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.

About: 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 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 Restoration Specialist at 855-443-3684 (1-855-4-IDENTITY).

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.

About: Lost Wallet

What is Lost Wallet Protection

Assists you in quickly and efficiently terminating and re-ordering wallet contents.

About: 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. SpotLight ID 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 Restoration Specialist at 855-443-3684 (1-855-4-IDENTITY).

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.

About: Full-Service Restoration

What is Full Service Restoration

ID Agent's Full-Service Identity Restoration service takes the burden off of your employees in the event that their identity is stolen. The ID Agent team goes beyond traditional credit restoration and can coordinate with banking institutions, law enforcement officials and legal representatives on your behalf.

Self-Service Identity Restoration is also available through ID Agent to assist by providing step-by-step instructions members can easily follow. The ID Agent team provides in-house, U.S.-based call center service with bilingual call center representatives, hearing impaired services and voice/e-mail/chat communication options.

Member Benefits

- Limited Power of Attorney
- Full-service restoration support from a certified identity theft restoration specialist
- Employees don't waste work productivity restoring their identities during business hours
- Reduce time, effort and stress associated with attempting to restore your identity on your own

Supporting Stats

200 hours is the average time spent with restoring an identity after an identity theft, most of which is spent during a typical work day.

About: 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 855-443-3684 (1-855-4-IDENTITY).

About: $1,000,000 Identity Theft Restoration Insurance Policy

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.

SPOTLIGHT ID

ID Agent provides threat intelligence and identity monitoring solutions to organizations and individuals. Its flagship product, Dark Web ID, delivers Dark Web intelligence to identify, analyze and monitor for compromised or stolen employee and customer data, mitigating exposure to clients' most valuable asset – their digital identity. Visit: www.idagent.com.

ID AGENT A Kaseya COMPANY