IDShield

Services and Features

IDShield offers one of the most comprehensive products on the market for protecting and restoring your identity. The following is a list of IDShield's specific services and features.

Identity Consultation Services

Members have unlimited access to identity consultation services provided by Kroll's Licensed Private Investigators. The Investigator will advise members on best practices for identity management tailored to the member's specific situation, and should there be an identity theft event, the investigator will recommend that a case be opened for restoration. Our IDShield advisors and licensed private investigators are available for all matters Monday-Friday, 7 a.m. to 7 p.m. Central Time at 888-494-8519. In the event of a personal identity theft emergency, advisors are available at 866-696-0927 to direct you to an investigator 24/7/365. All members are eligible to receive the following consultative services:

Privacy and Security Best Practice

- Consult on best practices for the use and protection of a consumer's Social Security number and Personal Identifying Information (PII)
- Provide consultation on current trends related to identity theft and fraud issues
- Discuss best practices for financial transactions
- Consult on best practices for consumer privacy
- Discuss tactics and best practices while shopping and communicating online
- Provide the knowledge to best protect the member from identity theft and to be aware of their rights under federal and state laws
- Help members interpret and analyze their credit report
- Take steps to reduce pre-approved credit card offers
- Consult with members regarding a public record inquiry or background search
- Credit Freeze consultation
- Consultation on common scams and schemes, including email and social media

Event-Driven Consultation Support

- Lost/stolen wallet assistance
- Data Exposure/Data Breach safeguards
- With member's permission, facilitate the placement of 90-day fraud security alerts with credit reporting agencies; if permission is not given, provide a list of contact phone numbers for placing fraud alerts

Alerts and Notifications

- Monthly identity theft updates to help educate and protect
- Data breach notifications

Pre-existing Stolen Identity Event Limitations — If the victim either had knowledge of, or reasonably should have had knowledge of, the misuse of his/her identity, credit, or other personal information based on information provided, or reasonably available, to the individual prior to enrollment in the program (each a "Prior Misuse"), such Prior Misuse or the consequences caused by it are not covered by the restoration services. However, individuals who have merely experienced the loss or unauthorized exposure of personal identifiers, including credit or debit card data, such as a data breach event, with no indication of actual misuse or identity theft resulting from that event, are not subject to the Prior Misuse exclusion hereunder.

Confirm Identity Fraud and Its Severity

- Social Security Number Fraud Detection — Use Social Security Number Skip Trace technique to investigate the member's name and Social Security Number in identifying potentially fraudulent activity; Skip Trace employs industry-unique database access afforded by the credentials of Kroll's Licensed Investigators
- Consultation and education on Criminal and Medical Identity Theft
- Discovery and consultation on Deceased and Minor Identity Theft
- Sex Offender Searches

Emergency Access—Identity Theft Emergency Situations

- Confirmed Check Fraud
- Criminal ID Theft
- Employment Fraud
- ID Theft Discovered through a Monitoring Alert or Otherwise
- Medical ID Theft
- Minor ID Theft
- New Account Opened
- Payday Loan
- Scam That Resulted in ID Theft
- IRS/Tax Fraud
- Utilities Fraud
- Passport, Personal Information Stolen while Traveling outside of U.S.

Pre-existing Stolen Identity Event Limitations — If the victim either had knowledge of, or reasonably should have had knowledge of, the misuse of his/her identity, credit, or other personal information based on information provided, or reasonably available, to the individual prior to enrollment in the program (each a "Prior Misuse"), such Prior Misuse or the consequences caused by it are not covered by the restoration services. However, individuals who have merely experienced the loss or unauthorized exposure of personal identifiers, including credit or debit card data, such as a data breach event, with no indication of actual misuse or identity theft resulting from that event, are not subject to the Prior Misuse exclusion hereunder.

Potential Emergencies

Call Type	Next Business Day	Potential Emergency	Not Fraud Related
Lost or Stolen Credit/Debit Card or Unauthorized Charges Member should place fraud alerts right away and let the Investigator follow up	●		
Breached/Compromised Data Precautionary Call Member should place fraud alerts right away and let the Investigator follow up	●		
Unconfirmed ID Theft*	●		
Confirmed Check Fraud		●	
Criminal ID Theft		●	
Employment Fraud		●	
ID Theft Discovered Through a Monitoring Alert or Otherwise		●	
Medical ID Theft		●	
Minor ID Theft		●	
New Account Opened		●	
Payday Loan		●	
Scam That Resulted In ID Theft		●	
IRS/Tax Fraud		●	
Utilities Fraud		●	
Passport, Personal Information Stolen while traveling outside of US		●	

*If identity theft is only suspected and not confirmed, Investigators on-call after hours will not be able to make the telephone calls necessary to confirm the probability of actual fraud. The best, and most productive, Investigator experience occurs during normal business hours when corporate fraud departments are open and conference calls may be conducted.

Consultation Services are limited to the solutions, best practices, legislation, and established industry and organizational procedures in place in the United States and Canada as determined beneficial or productive by a Kroll Licensed Private Investigator.

Privacy Monitoring

Black Market Website Surveillance (Internet Monitoring)

Monitors global black market websites, IRC (internet relay chat) channels, chat rooms, peer-to-peer sharing networks, and social feeds for a member's Personally Identifiable Information (PII), looking for matches of:

- Name

Pre-existing Stolen Identity Event Limitations — If the victim either had knowledge of, or reasonably should have had knowledge of, the misuse of his/her identity, credit, or other personal information based on information provided, or reasonably available, to the individual prior to enrollment in the program (each a "Prior Misuse"), such Prior Misuse or the consequences caused by it are not covered by the restoration services. However, individuals who have merely experienced the loss or unauthorized exposure of personal identifiers, including credit or debit card data, such as a data breach event, with no indication of actual misuse or identity theft resulting from that event, are not subject to the Prior Misuse exclusion hereunder.

- Date of birth
- Social Security Number
- Emails (up to 10)
- Phone numbers (up to 10)
- Driver's License number
- Passport Number
- Medical ID numbers (up to 10)

When an exact match for the monitored information is found, the member is alerted with an email notification. The detail of the alert can be accessed via the service portal dashboard.

Address Change Verification

Keeps track of a personal mailing address and alerts when a change of address has been requested through the United States Postal Service. An initial baseline report is provided of activity within the last 18 months, and monitoring thereafter provides alerts whenever a new change of address request is made. The detail of the alert can be accessed through the member dashboard on www.myidshield.com. This service can be accessed immediately by the member via the service portal dashboard.

Social Media Monitoring

Social Media Monitoring allows you to monitor multiple social media accounts and content feeds for privacy and reputational risks. You can set up monitoring for your Facebook, Twitter, LinkedIn and Instagram accounts to receive reports and alerts for content items such as image captions, posts, and comments. You will be alerted to privacy risks like the exposure of personally identifying information, including street address, date of birth, or Social Security number. Social Media Monitoring also searches for content that has the potential to create reputational risks, like foul language, drug and alcohol references, or discriminatory terms.

Security Monitoring

Black Market Website Surveillance (Internet Monitoring)

Monitors global black market websites, IRC (internet relay chat) channels, chat rooms, peer to peer sharing networks, and social feeds for a member's Personally Identifiable Information (PII), looking for matches of:

- SSN
- Credit card numbers (up to 10)
- Bank account numbers (up to 10)

When an exact match for the monitored information is found, the member is alerted with an email notification. The detail of the alert can be accessed through the member dashboard on www.myidshield.com.

Pre-existing Stolen Identity Event Limitations — If the victim either had knowledge of, or reasonably should have had knowledge of, the misuse of his/her identity, credit, or other personal information based on information provided, or reasonably available, to the individual prior to enrollment in the program (each a "Prior Misuse"), such Prior Misuse or the consequences caused by it are not covered by the restoration services. However, individuals who have merely experienced the loss or unauthorized exposure of personal identifiers, including credit or debit card data, such as a data breach event, with no indication of actual misuse or identity theft resulting from that event, are not subject to the Prior Misuse exclusion hereunder.

Court Records Monitoring

Detects criminal activity that may be associated with an individual's personal information, alerting them to signs of potential criminal identity theft. This service searches for online court records that match the member's name and date of birth from county courts, Department of Corrections (DOC), Administration of the Courts (AOC), and other legal agencies—approximately 350 million criminal records searched. Court records are sourced from county, state and federal data sources. County records are sourced from the 250 most populous counties along with arrest records, court records, correctional records and State Department records. If an incident appears associated with the member's information, they will be notified via alert.

Credit Monitoring

Members have access to continuous credit monitoring through Experian only. Monitoring can be accessed immediately by the member via the service portal dashboard. Credit activity will be reported promptly to the member via an email alert. Monitoring does not affect an individual's credit score, nor does it appear as a hard inquiry on his or her credit report when accessed by a third party. The credit monitoring service will alert members to activity up to and including new delinquent accounts, fraud alerts, improved account, new account, new address, new bankruptcy, new employment, new account inquiry, card over limit, deceased, liens and judgements, lost or stolen cards, major derogatory, new unconfirmed address, settlement, skip cannot locate, and new public records.

Pre-existing Stolen Identity Event Limitations — If the victim either had knowledge of, or reasonably should have had knowledge of, the misuse of his/her identity, credit, or other personal information based on information provided, or reasonably available, to the individual prior to enrollment in the program (each a "Prior Misuse"), such Prior Misuse or the consequences caused by it are not covered by the restoration services. However, individuals who have merely experienced the loss or unauthorized exposure of personal identifiers, including credit or debit card data, such as a data breach event, with no indication of actual misuse or identity theft resulting from that event, are not subject to the Prior Misuse exclusion hereunder.

Credit Inquiry Alerts

Members will be notified via email when a creditor requests their Experian credit file for the purposes of opening a new credit account. Alerts may also be triggered when a creditor requests a member's credit file for changes that would result in a new financial obligation, such as a new cell phone account, a lease for a new apartment, or even for an application for a new mortgage. Inquiry alerts can be helpful in determining when an identity thief is opening a new account without the member's authorization.

Monthly Credit Score Tracker

A monthly credit score from Experian that plots the member's score month-by-month on a graph. Upon enrollment and quarterly thereafter, members will be able to see how their credit scores have changed over time, along with score factors that provide insight into what events may have caused their specific credit score to change.

Payday Loan Monitoring

Alerts the subscriber when their personal information is associated with short-term, payday, or similar cash-advance loans. The service monitors 21,000 online, rent-to-own, and payday lender storefronts for unauthorized activity. An initial report is provided, and monitoring continues on a monthly basis. An alert is generated whenever new loans or inquiries are detected.

Minor Identity Protection

(Formerly Safeguard for Minors) Allows parents/guardians of up to 8 minors under the age of 18 to monitor for potential fraudulent activity associated with their child's SSN. Unauthorized names, aliases and addresses that become associated with a minor's name and date of birth may be detected. The service monitors public records in all 50 states, including real estate data, new mover information, property and recorder of deed registration, county assessor/record data, internet job site providers, state occupational license data providers, voter information, public records/court proceedings, bankruptcies, liens, and judgments. Parents/guardians are provided a baseline scan, subsequent alerts and notifications thereafter.

IDShield Vault

Members have access to a password manager as a part of their IDShield service. Members will be able to access a separate IDS Vault Dashboard where they will be able to store and manage their passwords as well as generate new, strong passwords. With a browser plugin installed, IDShield Vault will also autofill known passwords when browsing on the web. IDShield Vault also syncs across devices and provides secure auto backup.

Pre-existing Stolen Identity Event Limitations — If the victim either had knowledge of, or reasonably should have had knowledge of, the misuse of his/her identity, credit, or other personal information based on information provided, or reasonably available, to the individual prior to enrollment in the program (each a "Prior Misuse"), such Prior Misuse or the consequences caused by it are not covered by the restoration services. However, individuals who have merely experienced the loss or unauthorized exposure of personal identifiers, including credit or debit card data, such as a data breach event, with no indication of actual misuse or identity theft resulting from that event, are not subject to the Prior Misuse exclusion hereunder.

Identity Restoration

Licensed Investigators

Kroll's Licensed Private Investigators perform the bulk of the restoration work required to restore a member's identity to pre-theft status. The following list outlines Kroll's typical identity restoration process. Please note that each case is unique, and Kroll Licensed Private Investigators will typically address a variety of issues during a restoration case.

Within one business day of receiving a fully executed Limited Power of Attorney and copies of the Member's Social Security card, driver's license, identity theft police report and most recent utility statement—complete with the Member's current name and address—Kroll shall:

- Notify the Social Security Administration (SSA), the Federal Trade Commission (FTC), and the U.S. Postal Inspection Service in cases where there is evidence the U.S. Postal Service was used in connection with the suspected fraud
- Place/confirm that 90-day fraud security alerts have been placed with the three credit bureaus

Pre-existing Stolen Identity Event Limitations — If the victim either had knowledge of, or reasonably should have had knowledge of, the misuse of his/her identity, credit, or other personal information based on information provided, or reasonably available, to the individual prior to enrollment in the program (each a "Prior Misuse"), such Prior Misuse or the consequences caused by it are not covered by the restoration services. However, individuals who have merely experienced the loss or unauthorized exposure of personal identifiers, including credit or debit card data, such as a data breach event, with no indication of actual misuse or identity theft resulting from that event, are not subject to the Prior Misuse exclusion hereunder.

After receiving the Credit Authorization Form, Kroll shall:

- Order a copy of the Member's credit report
- Review credit history and document if fraud includes items such as:
    - Public records: liens, judgments, bankruptcies
    - Credit accounts: new and/or derogatory
    - Addresses
    - Prior employment
- Issue Fraud Alert and notification of fraud dispute—Work with affected financial institutions, collection agencies, check clearinghouse companies, landlords and property managers, and/or credit card companies, where warranted
- Issue Fraud Victim Statements—Work with all three credit bureaus to restore credit accuracy and place seven-year fraud victim statements with the permission of the victim

Where warranted, Kroll will:

- Search victim's local county criminal data to detect criminal activity being committed in member's name
- Use the U.S. Criminal Records Indicator to search a wide variety of national criminal databases
- Search victim's state's Department of Corrections records, court records, and arrest logs from numerous states
- Perform a driver license search using public records and commercially available data to find associated reports from numerous states
- Perform a Social Security trace to look for additional addresses that may be attached to the victim's name
- Perform a death indicator search using public records and commercially available data sources to determine if the victim has been reported as deceased for insurance fraud or other reasons
- Perform a check-clearinghouse search to determine if victim's name has been submitted as having been involved in fraudulent banking activities
- Notify the DMV and instruct victim on proper procedures in dealing with the DMV
- Notify and work with creditors who have extended credit due to misuse of the victim's identifying information
- Notify and work with the collection agencies of those creditors
- Notify and work with law enforcement personnel, both local and federal

If disputes are not resolved according to the victim's legal rights, Kroll may escalate disputes to the appropriate government/regulatory agencies, including:

- Federal Trade Commission
- State Attorney General office by state
- Consumer Financial Protection Bureau
- Association of Collection Professionals International
- Comptroller of the Currency
- Federal Reserve Bank
- Office of Thrift Supervision
- Office of the Inspector General
- Provide the additional assistance of investigators who can reasonably assist based on the victim's issues

In all cases, Kroll provides:

- Follow-up credit reports
- Subscriber updates

Pre-existing Stolen Identity Event Limitations — If the victim either had knowledge of, or reasonably should have had knowledge of, the misuse of his/her identity, credit, or other personal information based on information provided, or reasonably available, to the individual prior to enrollment in the program (each a "Prior Misuse"), such Prior Misuse or the consequences caused by it are not covered by the restoration services. However, individuals who have merely experienced the loss or unauthorized exposure of personal identifiers, including credit or debit card data, such as a data breach event, with no indication of actual misuse or identity theft resulting from that event, are not subject to the Prior Misuse exclusion hereunder.

Restoration Preparation

Benefit	Limited POA	No POA
Assist in organizing details of issues	●	●
Explain fraud victim's rights	●	●
Educate you on the process and your responsibilities	●	●
Assist in gathering and completing paperwork, including police reports	●	●
Send Fraud Packet to victim List of Contact Numbers (for immediate fraud alerts): Equifax Fraud Center • Experian Fraud Center • TransUnion Fraud Center • Federal Trade Commission • Social Security Administration • United States Postal Service	●	●
Issue Fraud Alert to all three credit repositories	●	●
Provide fraud victim assistance material	●	●
Assist you with questions as you work through the process	●	●

Restoration Process

Within 24 hours of receiving the signed Limited Power of Attorney, Kroll will:

Benefit	Limited POA	No POA
Issue Fraud Alert to Social Security Administration (SSA)	●	●
Issue Fraud Alert to Federal Trade Commission (FTC)	●	●
Issue Fraud Alert to U.S. Postal Service (USPS)	●	●

After receiving both signed Limited Power of Attorney and tri-merged credit report, Kroll will:

Benefit	Limited POA	No POA
Issue Fraud Victim statements and work with all three national repositories (Experian, TransUnion, Equifax) to restore credit accuracy	●	
Review credit history with you and verify if fraud includes items like: • Public Records (Liens, judgments, bankruptcies) • Credit Accounts (New and/or derogatory) • Address • Prior employment	●	●
Issue Fraud Alert to and work with affected financial institutions and credit card companies	●	

Whenever A Fraud Issue Warrants

Benefit	Limited POA	No POA
Determine if creditors extended credit due to misuse of your identifying information	●	
Confirm creditor contact information	●	
Contact creditors and collection agencies to dispute all fraudulent accounts	●	
Notify and work with the collection agencies of creditors holding fraudulent accounts	●	
Turn over any current accounts to fraud, requesting affidavits of documentation forwarded to you	●	
Search Criminal Data in your country of residence to look for criminal activity being committed in your name	●	
Search U.S. Criminal Records indicator to search a wide variety of national criminal databases	●	
Search Department of Motor Vehicles records in your state	●	
Perform a Social Security trace to look for additional addresses that may be attached to your name	●	
Perform a Social Security Death Index search to verify if you have been submitted to Social Security	●	
Determine if you have been submitted as having been involved in fraudulent banking activities	●	
Assist you in working with law enforcement personnel	●	
Use licensed attorneys where appropriate to perform these duties	●	
Offer additional assistance that can be reasonably provided based on your issue	●	●
Provide a list of attorneys who may be able to help you with legal issues—any subsequent relationship is exclusively between you and the attorney	●	●

Case Closing Process

Benefit	Limited POA	No POA
Provide a tri-merged credit bureau report follow up 120 days after resolution of your identity theft issues	●	
Update member	●	
Continue restoration until complete	●	
Responsibility for Kroll's Fraud Solutions Practice will cease when Kroll receives verification from you that the issue is resolved	●	●

Pre-existing Stolen Identity Event Limitations — If the victim either had knowledge of, or reasonably should have had knowledge of, the misuse of his/her identity, credit, or other personal information based on information provided, or reasonably available, to the individual prior to enrollment in the program (each a "Prior Misuse"), such Prior Misuse or the consequences caused by it are not covered by the restoration services. However, individuals who have merely experienced the loss or unauthorized exposure of personal identifiers, including credit or debit card data, such as a data breach event, with no indication of actual misuse or identity theft resulting from that event, are not subject to the Prior Misuse exclusion hereunder.

Theft Restoration Service Exclusions

The following are excluded from the Services:

Legal Remedy—Any Stolen Identity Event where the member is unwilling or unable to prosecute or otherwise bring a civil or criminal claim against any person culpable or reasonably believed to be culpable for the fraud or its consequences.

Dishonest Acts—Any dishonest, criminal, malicious or fraudulent acts, if the member(s) that suffered the fraud personally participated in, directed or had knowledge of such acts.

Financial Loss—Any direct or indirect financial losses attributable to the Stolen Identity Event, including but not limited to, money stolen from a wallet, unauthorized purchases of retail goods or services online, by phone, mail or directly.

Pre-Existing Stolen Identity Event Limitations—Any circumstance wherein the member had knowledge of, or reasonably should have had knowledge of a pre-existing Stolen Identity Event based on information provided to them prior to enrollment in the program.

Business—The theft or unauthorized or illegal use of any business name, DBA or any other method of identifying business (as distinguished from personal) activity.

Third Parties Not Subject to U.S. or Canadian Law—Restoration services do not remediate issues with third parties not subject to United States or Canadian law that have been impacted by an individual's Stolen Identity Event, such as financial institutions, government agencies, and other entities.

Pre-existing Stolen Identity Event Limitations — If the victim either had knowledge of, or reasonably should have had knowledge of, the misuse of his/her identity, credit, or other personal information based on information provided, or reasonably available, to the individual prior to enrollment in the program (each a "Prior Misuse"), such Prior Misuse or the consequences caused by it are not covered by the restoration services. However, individuals who have merely experienced the loss or unauthorized exposure of personal identifiers, including credit or debit card data, such as a data breach event, with no indication of actual misuse or identity theft resulting from that event, are not subject to the Prior Misuse exclusion hereunder.

IDShield Guarantee

Service Guarantee

We don't give up until your identity is restored.

We're confident in our ability to help protect your identity, but no one can prevent all identity theft. If you become a victim of identity theft while an IDShield member, we'll spend up to $5 million using Kroll's industry-leading licensed private investigators to do whatever it takes for as long as it takes to help recover and restore your identity to its pre-theft status.

You will have access to our U.S.-based Member Services agents during business hours and in emergency situations, 24 hours a day, 7 days a week, 365 days a year. And Kroll's Licensed Private Investigators are available to support you every step of the way.

Our industry-leading identity restoration experts are ready and waiting to help restore your identity. Unlike other providers in the market, we don't waste time retaining an insurer to restore your identity as we have a fully integrated partnership allowing Kroll's Licensed Private Investigators to handle your identity restoration needs.

We understand how important it is to be prepared for the worst. We are ready to take action immediately.

LegalShield®

IDS Services/Features (07/17)