IDENTITY THEFT PLAN ("Plan Services")

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. Members have access to member support agents and 24/7/365 for emergency situations. Kroll's Licensed Investigators will be available to answer questions regarding ID Theft and Fraud issues from 7am to 7pm central time, Monday through Friday excluding major holidays.

All Members are eligible to receive the following Identity Consultation 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 ID 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 ID Theft using 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 members
- Data breach notifications delivered to members

Confirm Identity Fraud and its Severity

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

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.

IDENTITY RESTORATION

All members are eligible to receive the following restorations services.

Licensed Investigators

Kroll's Licensed 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 Investigators will typically address a variety of issues during a restoration case.

Within 1 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

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 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

PRIVACY MONITORING – available to Member and Spouse

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
- 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.

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.

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.

SECURITY MONITORING --available to Member and Spouse

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.

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 - approx. 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, and new public records.

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 an application for a new mortgage.

Monthly Credit Score Tracker
A monthly credit score from Experian that plots the member's score quarter by quarter 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, pay day, 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 is provided on a monthly basis. An alert is generated whenever new loans or inquiries are detected.

MINOR IDENTITY PROTECTION (Family Plans only)
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 and includes; 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.

SERVICE GUARANTEE
If a Member becomes a victim of identity theft while an IDShield member, the Company will spend up to $5 million using Kroll's industry-leading Licensed Investigators to do whatever it takes for as long as it takes to help recover and restore a Member's identity to its pre-theft status. Company will spend an unlimited amount of time and money to fully restore a Member's identity.

IDENTITY 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.

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.