IDShield℠

IDShield National Plan Benefit Overview

IDShield is an industry leader in identity theft protection, monitoring and restoration services. Through IDShield, participants receive a comprehensive set of identity theft tools and professional services, backed by a team of licensed private investigators (LPIs) who work tirelessly to restore a participant's identity, should it ever become compromised. In addition, they provide proactive consultation services and support. That way, participants can focus on what matters instead of trying to resolve their identity theft issue on their own.

Restoration Services (IDShield Complete Restore)

Every few seconds, someone becomes a victim of identity theft. When it strikes, it's hard to know what to do or where to turn. Identity theft can lead to many types of fraud, including:

- Account takeover fraud
- New loan account fraud
- New credit account fraud
- Utilities account fraud
- Check fraud
- New cell phone fraud
- New bank account fraud
- Payday loan fraud
- Medical ID fraud
- Auto loan fraud
- Student loan fraud
- Tax refund fraud
- Employment fraud
- Government Benefits fraud
- Mortgage fraud

IDShield monitors participants' personally identifiable information (PII) from all angles. Identity and credit threat alerts are sent to the participant if any suspicious activity is found. If a participant's identity is stolen, IDShield provides full-service restoration and will restore the participant's identity to its pre-theft- status.

Dedicated U.S. Licensed Private Investigators:

IDShield has a team of U.S.-based, experienced LPIs. This license status allows them access to exclusive databases.

Our investigators' top-tier credentials include:

- Fair Credit Reporting Act (FCRA) certified
- Certified Fraud Examiners (CFE)

- Certified Identity Theft Risk Management Specialist (CITRMS)
- Certified Information Privacy Professional (CIPP/US)

If a participant has their identity stolen, one of our investigators will be directly assigned throughout the life of the case, creating a 1:1 relationship with the participant. The participant will have direct access -- via phone, email or our mobile app -- to their dedicated investigator throughout the identity restoration process.

Full Service Restoration: IDShield provides participants with a top-notch internal team of U.S.-based, professionally-licensed private investigators who will work tirelessly on behalf of the participant, their spouse, and/or their dependents (under the age of 26) to fully restore their identity to pre-event status- including pre-existing identity theft matters. No other company offers this high level of professional service. On top of fully comprehensive restoration and remediation, our experienced investigators provide one-on-one consultation and support to help prevent participants from becoming a victim of fraud or identity theft. Working with government agencies, financial institutions, credit bureaus, creditors, collection agencies and more, these investigators have the experience and credentials necessary to work on behalf of the participant and/or their eligible family members to restore their identity and to conduct fraud research that goes beyond what's on the surface.

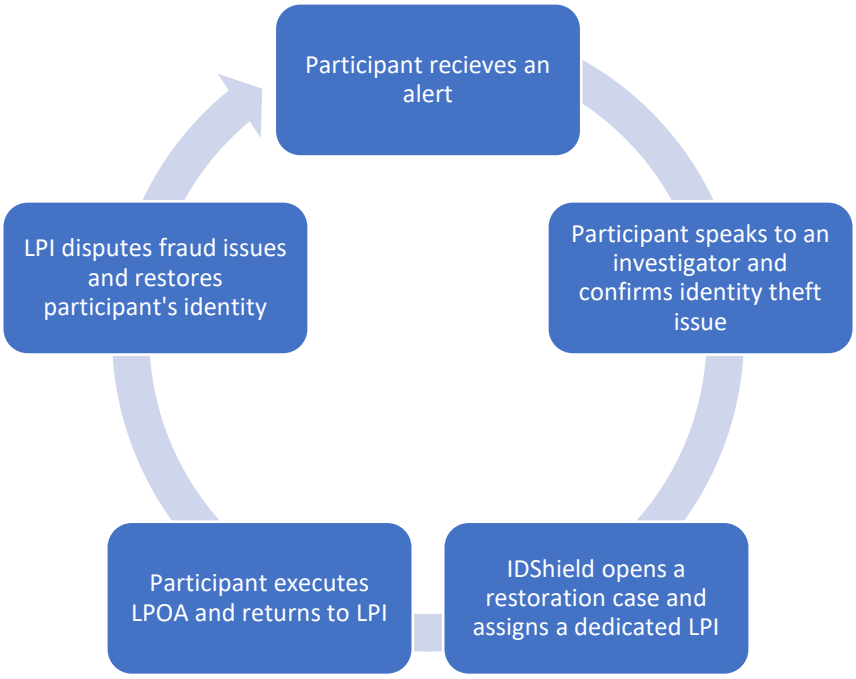
As part of the restoration process, the assigned LPI will:

- Organize details of open identity theft issues and search for other instances of identity theft
- Review with the participant their credit history and verify if fraud includes items such as: public records (liens, judgments, bankruptcies), credit accounts (new and/or derogatory), addresses, and prior employment
- Explain the participant's rights, process and responsibilities involved
- File fraud alerts and disputes with reporting agencies and creditors as needed
- Obtain a Limited Power of Attorney authorization, which allows the LPI to take actions on behalf of the participant. For example: issue a Fraud Alert to all three credit bureaus, and notify the Social Security Administration (SSA), Federal Trade Commission (FTC) and U.S. Postal Service (USPS) Work directly with financial institutions and credit card companies.

Throughout the restoration process, the licensed private investigator will provide step-by-step guidance and updates. Backed by a $5 Million Service Guarantee, the participant's identity will be restored to pre-theft status, and is continually monitored for future identity threats.

Restoration Verification: Upon completion of the restoration, IDShield will complete a verification 120 days after a case is resolved to ensure the participant has not been targeted again. For the case to be fully closed, confirmation is needed from the participant and the

assigned investigator. If a threat is uncovered at any point during this time, the restoration process will resume.



In-Depth Fraud Investigation: IDShield combines information and databases with proprietary investigative methods to conduct fraud investigations. Our highly-credentialed, investigators can quickly identify signs of fraudulent activity, as well as its source, to help stop the spread of identity theft. This includes all types of identity fraud, including medical fraud.

$5 Million Service Guarantee: IDShield will do whatever it takes for as long as it takes to restore a participant's identity back to its pre-theft status. We provide an industry-leading $5 Million Service Guarantee.

New! $1 Million Identity Fraud Reimbursement:

The Identity Fraud Reimbursement Policy coverage provides reimbursement for expenses and legal costs incurred by the participant and or the participant's spouse/eligible dependents. This policy covers expense reimbursement for the following events if a stolen identity event or unauthorized electronic funds transfer is reported:

• Costs for refiling, notarization, credit reports, public record changes, travel, elder/child care, expedition of credit/debit card replacement, or accountant fees.

• Lost wages

• Legal defense fees and expenses

• Unauthorized Electronic Fund Transfer Reimbursement

Monitoring and Detection Services (IDShield Detect and Alert)
IDShield is there to monitor a participant's credit and identity from every angle. From credit scores and driver's license numbers to social media accounts and beyond, IDShield's 360 Degree approach leaves nothing to chance. When a threat is detected, IDShield will send an immediate alert to the participant via email or push notification on the IDShield mobile app.

New! Auto-Monitoring:

IDShield's auto-monitoring provides participants monitoring services directly upon enrollment. Using the participant's full or partial Social Security number (SSN), and date of birth, the SSN, along with other member-provided personally identifiable information is then automatically monitored.

The following information is required for participants to be enrolled in auto-monitoring:

- Date of Birth
- Full or partial SSN
- First Name
- Last Name
- Complete Home Address

The following services will be automatically turned on at the time of enrollment:

- Credit Monitoring
- Public Records Monitoring
- Court Records Monitoring
- Sex Offender List Monitoring
- Address Change monitoring
- Payday loan monitoring
- High Risk Application and Transaction Monitoring
- Dark web Internet Monitoring

The participant will need to create an account on the member portal, myidshield.com, to update their demographics, input their full SSN (if not provided), and any additional PII they would like monitored. The participant will then be prompted to answer authentication

questions. Once the participant has successfully completed the authentication, they can view the details of alerts and download the IDShield mobile app.

Comprehensive Dark Web Internet Monitoring: IDShield's Comprehensive Dark Web Monitoring provides extensive monitoring of the participant's personally identifiable information (PII) across the Dark Web, a series of black market websites where criminals purchase personal information.

PII monitored includes:

- Investment Account Number – **New!**
- Mother's Maiden Name – **New!**
- Usernames – **New!**
- National Provider Identifier (NPI) Number – **New!**
- Full Name
- Date of Birth
- Social Security Number
- Driver's License
- Passport Number
- Phone Numbers (up to 10)
- Bank Account Numbers (up to 10)
- Credit/Debit Card Numbers (up to 10)
- Retail Card Numbers (up to 10)
- Medical ID Numbers (up to 10)

We review thousands of websites and data points across the Dark Web to ensure participants' information is not exposed. If participant information is found, the participant will receive an alert.

Identity Threat Alerts: If any PII is found through IDShield's monitoring services, an identity threat alert is sent to the participant via email and through push notifications on the IDShield mobile app. The participant can review the alert with an investigator for further assistance. If no threats are found you will receive a monthly 'no-activity' notice via email.

Credit Threat Alerts: If any changes or updates are found on the participant's credit report, credit threat alerts are sent via email and through push notifications on the IDShield mobile app. The participant can review the alert with an investigator for further assistance.

New! Hard Credit Inquiry Alerts:

Hard credit inquiry alerts continuously monitor a participant's Experian credit report for new hard inquiries and triggers notifications to the participant in real-time, when the inquiry is made by the creditor. The alert is triggered when a participant, or someone using their PII, completes

an application that includes a credit check such as when applying for a loan, mortgage, or credit card. Events leading to a hard inquiry include:

• Auto Loan Inquiry

• Bank/Credit Card Inquiry

• Business Loan Inquiry

• Home Equity Loan Inquiry

• Installment Loan Inquiry

• Auto Lease Inquiry

• Mortgage Loan Inquiry

• Recreational Merchandise Inquiry

• Rental Inquiry

• Retail Loan Inquiry

• Student Loan Inquiry

• Utility Inquiry

The participant can then review the alert with an investigator who will review the inquiry further.

Continuous Credit Monitoring:

IDShield provides plans with all 3 credit bureau (Experian, Equifax and Transunion) and 1 credit bureau (Experian) monitoring.

IDShield continuously monitors the participant's credit report for the following:

- Delinquent Status
- Fraud or Victim Statement
- New Inquires and Trades
- Public Record/Trade Line Bankruptcy/Other Major Derogatory
- Card Over Limit
- Participant Noted as Deceased
- Liens and Judgments
- Reported Lost or Stolen Card
- New Address
- Settlement
- Missing Address

If discrepancies are found, the participant will receive an alert. As part of the restoration process, a credit report from all three credit bureaus will be provided if the participant's identity is compromised.

Monthly Credit Score Tracker: The participant's Experian credit score is tracked monthly and automatically updated and displayed on the IDShield mobile app and member dashboard.

Credit Freeze and Fraud Alert Assistance: IDShield LPI will provide the participant assistance with placing a credit freeze and/or fraud alert on their credit reports in the event of a breach or other identity theft incident.

New! **High Risk Application and Transaction Monitoring:** IDShield monitors the largest proprietary database of new account application data to detect potentially fraudulent new accounts when an application is applied for. This allows fraud detection up to 90 days earlier than traditional credit monitoring services. Exclusive to IDShield is the ability to electronically send a message back to the issuing organization that the activity is not the participant. We monitor hundreds of billions of data points for applications such as:

- Checking/Savings/Brokerage Accounts
- Wireless and Utility Accounts
- Auto and Home Loans
- Credit Card Applications
- Check Reorders
- Retail Charge Accounts
- Payday Loans

IDShield also monitors and alerts participants for transactions that appear to been unusually risky or have a high potential of identity theft in a number of categories like Banking, Finance and Brokerage, Credit, Benefits & Payroll, and Insurance & Healthcare.

New! **Public Records Monitoring:** IDShield now offers expanded public records monitoring of over 78 billion public records and growing, which in addition to criminal records, professional and business licenses, pilot licenses, merchant vessels, registrations (DEA, vehicle, concealed weapons, and voter registration), residences, lease history, national property and deeds, Social Security Death Index, Social Security number verifiers, phones, aliases, criminal records, and more.

Court Records Monitoring: IDShield searches online court records for the participant's name and date of birth. We search over 350 million criminal records including county courts, Department of Corrections (DOC), Administration of the Courts (AOC), local, state and federal data sources and other legal agencies.

Payday Loan Monitoring: IDShield provides extensive non-credit loan monitoring for short-term payday or similar cash advance loans. Non-credit loan sources such as online, rent-to-own or payday lender storefronts are monitored for unauthorized activity.

New! Telecom Monitoring: IDShield monitors databases with more than 1.5 billion phone records for any new landline, wireless, or VOIP telecom accounts associated with a participant's identity.

Address Change Monitoring: IDShield monitors the participant's home address with the United States Postal Service and sends an alert if a change of address has been requested.

Child Monitoring: IDShield will monitor up to 8 dependent children under the age of 18, for potential fraudulent activity associated with the participant's child's Social Security number (SSN). The service monitors public records in all 50 states, including real estate data, public records/court proceedings, bankruptcies and liens. Parents/guardians are provided a baseline scan, subsequent alerts, and notifications if a minor child's data is found. Children ages 18-26 are covered under the plan for consultation and restoration services if they become a victim of identity theft.

Social Media Monitoring: IDShield monitors popular social media platforms: Facebook, LinkedIn, Twitter, and Instagram for information that may put the participants' privacy at risk, such as home address, email address, date of birth and Social Security number. Additionally, IDShield alerts participants to reputational risks within their content feeds such as instances of vulgar, harmful, or threatening and/or sexual language, drug and alcohol references and discriminatory language.

New! Participants can control the sensitivity level of their alerts based on content and subjects including Geotargeting, language, etc.

IDShield Vault: The IDShield Vault is an industry-leading password protection manager with military-grade encryption. It allows participants to manage and generate strong and secure passwords. With a browser plugin installed (Chrome, Firefox, or Safari), IDShield Vault will also autofill known passwords when browsing on the web and sync across devices providing secure auto backup. IDShield Vault is also available in the mobile app.

Consultation Services (IDShield Identity Consultation Support)
Participants have unlimited access to consultation with a LPI when they have questions about a recent data breach, an identity-related issue or any other concern, such as receiving a suspicious email or phone call, notification of a change on their credit report, or concerns about proactively protecting their personal information. A participant doesn't have to be a victim of identity theft to take advantage of consultation services.

24/7 Emergency Assistance: In the event of an identity theft emergency, IDShield provides emergency access for participants to reach a licensed private investigator 24/7/365, ensuring they can get help right away.

Exclusive Identity Insights and Tips: IDShield provides participants with best practices for use and protection of their PII including insights and tips directly from our investigators.

Social Security Skip Trace: IDShield has the unique ability to uncover further fraud and potential identity theft by using a SSN Skip Trace method. Our investigators have access to specialized tools that allow them to conduct a quick, thorough search for further evidence of potential identity theft beyond what is found through an initial alert.

Lost/Stolen Wallet Support: Losing a wallet or purse containing sensitive information can be scary, but IDShield investigators are there to assist. They will provide guidance and work with the participant to review what may have been lost or stolen. The investigators will also use their access to special databases to provide a comprehensive investigation to determine if there was any misuse of the participant's identity after the event. If any discrepancies are found the LPI will open a restoration case.

Solicitation Defender:

Fraudsters and identity thieves use many methods to obtain PII. Reducing mail and phone solicitations helps reduce the risk of thieves finding personal information such as a participant's mailing address. Links are available on the web dashboard to remove PII from solicitation services.

Additionally, participants can call and speak directly with a LPI FOR advice and assistance to reduce unsolicited offers for credit cards and insurance and for assistance WITH REMOVING fraudulent information from public records sources.

NEW! Medical Data Reports: IDShield provides links to 3 sources of medical data reports (including MIB Consumer file) that a participant can pull to review for inaccurate or potentially fraudulent information. If there are any questions, they can call into IDShield for consultation.

Financial Account Safeguard: Participants can seek consultation on what actions to take if they notice an unidentified transaction and consultation on safeguarding their financial accounts. If an unknown transaction was made, a LPI will leverage specialized tools to search for suspicious activity involving the participant's PII.

Sex Offender Search: New! Participants can now search for sex offenders within an adjustable radius of their home address and receive alerts when new sex offenders move in.

Data Breach Notifications: Information about large and high publicity data breaches is provided to participants via email and also included on the member portal, myidshield.com.

IDShield Mobile App: The IDShield mobile app makes it easy for participants to access their benefits. Participants simply login with the user name and password they created for myidshield.com to access this app.

Features Include:

- Push notifications for identity threat and credit Threat alerts
- Monthly credit score tracker
- Direct Access to IDShield investigators
- 24/7 emergency assistance
- Access to IDShield's password manager, IDShield vault
- ABILITY TO Track and edit monitored information

Review of Restoration Case status and history

Review of LPI Consultation History

This app is available both on android and apple devices and for iPhone users, Touch ID Support is available for applicable devices.

Language Support: IDShield's investigators are staffed to provide language support in English, Spanish, and French. In addition, we have real-time language support for over 100 languages to ensure effective communication with all participants.

Live Member Support: IDShield's Participant Services team is available for participant support from 7 a.m. to 7 p.m. CT, Monday-Friday.

IDShield is a product of LegalShield and provides access to identity theft protection and restoration services. 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.