IDShield™

IDShield Plan Overview

Accessing Identity Theft Services

To receive identity theft consultation and restoration services, call 888-494-8519. For questions about the plan, contact Member Services at 1-888-807-0407 from 7 a.m. CT — 7 p.m. CT, Monday — Friday. For emergency after hours support call 1-866-696-0927.

Who is Covered

The IDShield Individual Plan covers the participant (employee).

The IDShield Family Plan covers the participant (employee), participant's spouse/partner, dependent children under the age of 26 and dependent parents.

Dependent children ages 18-26 and dependent parents of the participant or participant's spouse/domestic partner are eligible for consultation and restoration services only. Monitoring services are not available for dependent parents and dependent children ages 18-26. A dependent parent is defined as an adult parent that 1. Lives in the home of the participant/participant spouse, 2. Resides in a care facility or 3. The participant/participant's spouse has a durable power of attorney for the parent.

What Services Are Covered

The IDShield plan includes the following covered services:

Restoration Services

$3 Million Identity Fraud Protection Plan

IDShield provides a $3 million identity fraud protection plan, provided by a leading national carrier.

This covers costs incurred as a result of identity theft – such as:

- Lost Wages
- Travel Expenses
- Elder and Child Care
- Initial Legal Consultation
- Certified Public Accountant Costs
- Stolen Funds from Unauthorized Electronic Funds Transfers
- Financial Loss from 401Ks and HSAs

Full-Service Restoration

If an identity theft event does occur, our Licensed Private Investigators will do whatever it takes for as long as it takes to restore a participant's identity to its pre-theft status. The investigator will work on a participant's behalf to resolve the issue by working with the appropriate government agencies, financial institutions, credit bureaus and collection agencies. No other company offers this high level of professional service.

With the IDShield Family plan, restoration services are provided to dependent children aged 18-26 and dependent parents of the participant and/or participant's spouse/domestic partner.

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
  - — 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. Authorized as a Limited Power of Attorney, the assigned LPI can then:
  - — Issue a fraud alert to all three credit bureaus.
  - — Notify the Social Security Administration (SSA).
  - — Notify the Federal Trade commission (FTC).
  - — Notify the U.S. Postal Service (USPS).
  - — Work directly with financial institutions and credit card companies to resolve any disputes.

Throughout the restoration process, the Licensed Private Investigator will provide status updates and ensure the participant's identity will be restored to its pre-theft status.

Licensed Private Investigators

Participants have access to consultation services provided by our Licensed Private Investigators. If a participant experiences an identity theft event, one of our investigators will walk them through their issues with one-on-one advice tailored to the specific situation. Participants will have access to an assigned and dedicated investigator throughout the restoration process. All Licensed Private Investigators are licensed in the state of Oklahoma.

Our investigators' credentials include:

- Fair Credit Reporting Act (FCRA) Certified
- Certified Identity Theft Risk Management Specialist (CITRMS)
- Certified Credit Scoring Specialist (CCSS)
- Certified Credit Report Reviewer (CCRR)

Monitoring and Detection

Address Change Monitoring

IDShield monitors participants' address history in the United States Postal Service through the National Change of Address database, providing an 18-month snapshot of the nearly 40 million Americans who move each year. This service scans for change of address requests and sends a notification if participant information appears in the database.

Application Alerts

For certain types of account applications, third parties will take participants' information, compare it to public records and return a fraud score. IDShield scans a national ID verification database to determine if a new account application has been submitted with participants' information. We continuously monitor to see if any new accounts or transactions appear.

Auto-Monitoring

IDShield's auto-monitoring provides participants with monitoring services directly on the effective date of the plan. Using the participant's full or partial Social Security Number (SSN), name, address and date of birth provided at time of enrollment, the participant's identity is automatically monitored. During account activation, participants are encouraged to provide further information to enable the full monitoring services the plan provides. To activate their account, participants will be asked two questions about their credit history to successfully authenticate their account and confirm their identity.

The following services are available for auto-monitoring:

- Credit Monitoring
- Dark Web and Internet Monitoring
- Court Records Monitoring
- Public Records Monitoring
- Address Change Monitoring

Only the named participant is subject to auto monitoring. Spouse and dependent child monitoring will require separate set-up by accessing the participant portal.

Child Monitoring

With the IDShield Family Plan, we'll monitor dependent children under the age of 18. Participants receive an alert if their child's SSN is used to create any new accounts or included in credit applications, loans, court documents, etc.

Continuous Credit Monitoring

IDShield provides 3 credit bureau monitoring (Experian, Equifax and TransUnion). Lenders, creditors and many businesses check and submit data to go on credit reports. If changes or inquiries are made, participants will receive an instant alert.

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

- Delinquent Account
- New Address
- New Tradeline
- Settlement
- Card Over Limit
- Lost or Stolen Card
- Participant Noted as Deceased
- Fraud or Victim Statement
- Bankruptcy
- Liens and Judgments
- New Employment
- New Collection

Court Records Monitoring

IDShield can determine if a participant's identity is associated with a criminal act by monitoring court records connected to their name, SSN and date of birth. Criminals can fraudulently use stolen identities, causing the victim's information to falsely appear on citations, arrest records, felonies, traffic offenses and convictions. IDShield monitors millions of dockets from the Administration of the Courts, the Department of Corrections, county courts and other legal agencies in search of participant data. If a match is found, the participant will receive an alert with the details.

Credit Threat Alerts

IDShield monitors for changes or updates found on the participant's credit report(s) in real time. We pull data from over 200 million files that represent nearly every credit active consumer in the United States.

Dark Web and Internet Monitoring

Billions of records are for sale on the dark web, so real-time monitoring is vital. IDShield's dark web and internet monitoring provides extensive scans of online sources for identity data and sends participants real-time alerts if their PII is found. IDShield reviews thousands of websites and data points across the dark web to see if participant information has been exposed.

We monitor the following:

- Auto Pawns/Title Pawns
- Bank Account Numbers
- Buy Here/Pay Here Auto Loans
- Credit/Debit/Retail Card Numbers
- Cryptocurrency Wallets
- Date of Birth
- Driver's License Number
- Enhanced Sub-Prime Loans
- Full Name
- Gamer Tags
- Investment Account Numbers
- Mailing Address
- Medical ID Numbers
- Mother's Maiden Name
- National Provider Identifier Number
- Passport Number
- Phone Numbers
- Rent-to-Own Applications
- Social Security Number
- Telecom Account Applications
- Username and Password Combinations

Deceased Family Monitoring

IDShield provides deceased family member monitoring for both a deceased spouse and a deceased child. For a deceased spouse added to the plan prior, we will monitor their PII and SSN on the Dark Web and provide Court Record Monitoring. If the spouse was added to the plan after they have become deceased, we will monitor their SSN on the Dark Web. For a deceased child we will monitor their SSN on the Dark Web.

Financial Account Monitoring and Alerts

IDShield monitors participants' financial accounts including credit cards, checking, savings, 401k, 403 (b), 457 accounts, loans and more for any discrepancies. Participants will receive alerts notifying them of financial withdrawals, balance transfers and large purchases on financial accounts, if a transaction is made outside of a set monetary amount. We also will list the most recent financial transactions and detect reoccurring payments which can be viewed as subscriptions.

High Risk Application and Transaction Monitoring

Financial institutions use specific technology to verify the identity of new account holders before processing high-risk transactions. IDShield monitors these processes to determine if details for a new bank account or large money transfer are associated with a participant's personal data. Our application and transaction monitoring can potentially catch identity theft 90 days faster than traditional credit monitoring alone. Furthermore, IDShield can better secure a participant's online financial records by monitoring unauthorized use of username and password combinations used for online banking or insurance accounts. This service monitors processes related to:

- Instant Credit Applications
- Financial Account Updates
- Credit Line Increases
- Money Transfers
- Activity on New Accounts
- Customer Payment Activity
- Online W-2 Access
- Online Prescription Management
- Fund Transfers

Identity Threat Alerts

Participants receive an alert via email or push notification on the IDShield mobile app if their information is found online. Alerts contain details on the threat, including links to where the exposure occurred – giving participants the opportunity to look over the information to either dismiss the notification or escalate the issue with our Licensed Private Investigators.

Instant Hard Credit Inquiry Alerts

Credit report inquiries are created when a participant's PII is used to apply for bank/credit cards, utility or rental query or many types of loans – including home, auto, business, mortgage, home equity or student loans. IDShield notifies participants when their information appears on these reports, empowering them to take action if their data has been exposed by reviewing the alert with an investigator.

Monthly Credit Score Tracker

The credit score tracker gives participants the ability to watch their Experian credit score on a monthly basis with a map that shows a 12-month historic view of their credit trends from the past year – beginning when the service was first activated.

Payday Loan Monitoring

IDShield provides non-credit loan monitoring for short-term payday or similar cash advance loans. We screen online, rent-to-own and payday lender storefronts for unauthorized activity.

Public Records Monitoring

IDShield monitors over 78 billion public record reports from more than 10,000 diverse sources to screen for 34 different pieces of PII – including name, address, phone number, email, SSN and more. The records contain the public, private and regulated data of over 283 million U.S. consumers which are checked for matches of participant information.

These reports include details on:

- Bankruptcy
- Motor Vehicle Records
- Driver's License Records
- Criminal Records
- Business Licenses
- Tax Assessor Records
- Residencies
- Lease History
- Registrations
- Deeds

Sex Offender Monitoring and Alerts

Participants can learn if a registered sex offender lives near them. They'll also receive alerts when a new offender moves into their neighborhood, out of their neighborhood or if someone in their neighborhood becomes registered. Participants can search within a five-mile radius of their home address.

With sex offender search, participants can:

- View sex offender details.
- Search using an adjustable radius of their home address.
- Receive alerts when a sex offender moves nearby.

Sub-Prime Monitoring

Sub-prime monitoring searches transaction data for rent-to-own, buy-here pay-here auto dealers, title pawn and sub-prime loan applications. Participants will be notified when new transactions are discovered.

Telecom Monitoring

IDShield monitors phone number history associated with an individual, as well as any phone number changes with a database of more than 1.2 billion landlines and mobile phones to assure participants that their phone number is not being redirected.

Username/Password (Credentials) Monitoring

IDShield monitors the internet for instances where a participant's username and password credentials have been exposed. When these are found together online, it presents a strong indication that their online accounts have been compromised. The service continuously scans for a participant's username/password combinations and will alert the participant with details so they can follow up and change their login information on any accounts that use the exposed credentials. When a monitored email is found on the Dark Web, participants will also have the option to view the password, after an email verification process, found associated with the monitored email address(es).

Online Privacy and Reputation Management

Anti-Malware Protection

IDShield's Maximum Security protection from Trend Micro, uses cloud-based AI technology to deliver highly effective and proactive protection against ever-evolving malware infections. As part of this protection, we provide a folder shield that limits access to important files and folders and can prevent ransomware from maliciously encrypting these files and Pay Guard, a protected web browser that adds an extra layer of protection when banking or shopping online.

The IDShield Individual Plan provides protection for up to three devices and the IDShield Family Plan provides protection for up to 15 devices.

System Requirements: Windows Operating Systems: Microsoft® Windows® 7 (all versions) with Service Pack 1 (SP 1) or later, Microsoft® Windows® 8.1 (all versions), Microsoft® Windows® 10 (Windows IOS and ARM processors only supported by IDShield Endpoint Anti-Malware on Microsoft® Store). Mac Operating Systems: Apple® macOS 10.14 to 10.15 and macOS11 Big Sur, Chrome OS Operating System: Chrome OS 79 or higher (Chromebooks only supported by IDShield Endpoint Anti-Malware on Chrome Web Store), Android Operating Systems: Android 4.1 or later. IOS Operating Systems: iOS 9 or later. 64-bit device required for latest version.

Cyberbullying Protection

If any covered participant is being bullied, online or face-to-face, we will connect them to local agencies/ authorities, school administrators and counselors and provide guidance on how to navigate the situation and reduce the impact of bullying on the victim.

Data Broker Site Management

With our reputation management service, participants can learn how to remove their personal information from data broker sites such as Whitepages, Instant Checkmate, Spokeo, among others.

Mobile Security

IDShield's mobile security from Trend Micro provides protection from ransomware, potentially dangerous and harmful websites, unsafe Wi-Fi networks, and more. Participants can even track, lock, and/or wipe a lost or stolen device.

System Requirements: Android Operating Systems: Android 4.1 or later. IOS Operating Systems: iOS 11 or later. IPadOS 13.0 or later. 64-bit device required for latest version.

Online Parental Controls

IDShield's maximum security protection from Trend Micro allows participants to set parental controls and content filters to monitor and block what web pages can be viewed, and schedule specific timeframes for when their children can browse the web.

System Requirements: Windows Operating Systems: Microsoft® Windows® 7 (all versions) with Service Pack 1 (SP 1) or later, Microsoft® Windows® 8.1 (all versions), Microsoft® Windows® 10 (Windows IOS and ARM processors only supported by IDShield Endpoint Anti-Malware on Microsoft® Store). Mac Operating Systems: Apple® macOS 10.14 to 10.15 and macOS11 Big Sur, Chrome OS Operating System: Chrome OS 79 or higher (Chromebooks only supported by IDShield Endpoint Anti-Malware on Chrome Web Store), Android Operating Systems: Android 4.1 or later. IOS Operating Systems: iOS 9 or later. 64-bit device required for latest version.

Online Privacy Management

IDShield provides consultation and guidance on ways participants can protect their privacy and Personally Identifiable Information across the internet and on their smart devices. Our certified and Licensed Private Investigators provide unlimited consultation on how to switch to easy-to-use and privacy-conscious alternatives to well-known software such as Google search, Gmail, Facebook, and Amazon. We will provide step-by-step advice and consultation to participants on how to take control of their online privacy by showing them how to:

- Delete unused online accounts
- Delete unused apps from their mobile phone
- Audit third-party app access to personal information
- Ensure their browser isn't tracking them
- Delete unused software on their computer
- Remove data from public records sites (Intelius, MyLife, BeenVerified, etc.)
- Reset and recycle (or donate) unused devices (mobile, PC)

IDShield's identity theft specialists also provide anti/cyberbullying, password, and privacy management consultation for:

- Data broker sites (Spokeo, MyLife, etc.)
- Social media platforms (Facebook, LinkedIn, Twitter, Instagram and YouTube)
- Voice assistance devices (Alexa, Google, etc.)
- Online browsers (Brave, Ghost, etc.)
- Smart TVs
- Password management services

Online Privacy Settings Management

Our reputation service allows participants to control their privacy settings across multiple platforms.

Password Manager

IDShield's password manager from Trend Micro allows participants to create strong and unique passwords and safely secure them. The password manager can identify weak passwords and change them with unique, tough-to-hack passwords. The IDShield Individual Plan provides one password manager license and the IDShield Family Plan provides six password manager licenses.

Windows Operating Systems: Microsoft® Windows® 7 (all versions) with Service Pack 1 (SP 1) or later, Microsoft® Windows® 8.1 (all versions). Microsoft® Windows® 10 (all versions). Edge browser not supported. Mac Operating Systems: Apple® macOS 10.12 to 10.14, Android Operating Systems: Android 5.1 or later. iOS: iOS 11.0 or later. 64-bit device required for latest version.

Reputation Management

IDShield's reputation management service allows the participant to scan their social media accounts including Facebook, Twitter, Instagram and TikTok for existing content that could be damaging to their online reputation. Participants will be notified of old accounts and high-risk posts and images, and will have the ability to review and the choice to remove flagged content for their personal accounts. IDShield's Family Plan provides this service to both the participant and the participant's spouse.

Reputation Score

A reputation score is provided based on content and photos found on scanned social media accounts. Tips to improve the participant's score are provided along with social posts and photos that were flagged as part of the scan. Participants will have the option to review flagged content and remove content from their personal accounts to improve their score.

Social Media Monitoring

IDShield monitors the participant's Facebook, Twitter, YouTube, LinkedIn and Instagram accounts to see if personal information has been exposed through image captions, posts and comments. Participants will be notified if their social content presents reputational risks such as foul language, drug references or discriminatory terms. Participants can control the sensitivity level of their alerts based on options chosen in their account settings - including categories for profanity, violence and more.

IDShield's Family Plan allows both the participant and the participant's spouse as well as their dependent children under the age of 18 to also monitor their social media accounts.

VPN Proxy One

IDShield's Virtual Private Network (VPN) Proxy One from Trend Micro™ utilizes bank-grade data encryption to prevent a participant's incoming and outgoing internet traffic from being tracked, hacked or censored. It turns a public hotspot into a secure Wi-Fi. The IDShield Individual Plan provides protection for up to 3 devices and the IDShield Family Plan provides protection for up to 15 devices.

System Requirements: Windows Operating System: Microsoft® 10 RS3 and above, Mac Operating Systems: Apple® macOS 10.12 and above, Android Operating Systems: Android 5.X and above, iOS Operating Systems: iOS 9.X and above.

Consultation Services and Support Tools

24/7 Emergency Assistance

In the event of an identity theft emergency, IDShield provides emergency access to live support 24/7, ensuring participants can get help right away.

Credit Counseling and Education

IDShield's identity theft specialists can provide one-on-one education to help participants understand their valuable credit rating and actions that are likely to have an impact on their credit score. They can also provide counseling on debt management, financial budgeting, credit score health and more.

Credit Freeze and Fraud Alert Assistance

IDShield's investigators 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. If their identity is stolen, the LPI will issue fraud alerts to all three credit bureaus and with reporting agencies and creditors as needed.

Language Support

IDShield's investigators can provide language support in English, Spanish and French.

Live Member Support

IDShield's identity theft specialists, Licensed Private Investigators and Customer Care teams are available from 7 a.m.-7 p.m. CT Monday-Friday. Identity theft specialists are also available 24/7 for identity theft emergencies.

Lost/Stolen Wallet Support

Losing a wallet can be stressful, but our investigators are there to assist. We offer guidance to determine what may have been stolen and provide support for any resulting identity theft.

Medical Data Report

Our site provides a link to sources of medical data reports. Participants can retrieve and review these reports for inaccurate or fraudulent information.

Solicitation Reduction

Reducing mail and phone solicitation helps lower the risk of thieves finding personal information to exploit. Our identity theft specialists are available to provide advice and assistance to reduce the number of unsolicited offers for credit cards and insurance participants receive.

Pre-Paid Legal Services, Inc. ("PPLSI") provides access to identity theft protection and restoration services through its product IDShield. IDShield plans are available at individual or family rates. A family plan provides monitoring services for eligible dependent children under the age of 18 of the Named Member or Named Member's spouse or domestic partner. Consultation and Restoration Services are available for eligible dependent children under the age of 26 and dependent parents. For complete terms, coverage, and conditions, please see an identity theft plan. All Licensed Private Investigators are licensed in the state of Oklahoma. An Identity Fraud Protection Plan ("Plan") is issued through a nationally recognized carrier. PPLSI is not an insurance carrier. This covers certain identity fraud expenses and legal costs as a result of a covered identity fraud event. See a Plan for complete terms, coverage, conditions, limitations, and family members who are eligible under the Plan.

US_BU_NP_IDS_PR_EN_BenefitOverviews_3B_v1_082823