

IDENTITY THEFT AND CYBER THREAT PROTECTION



Identity Protection Services (IPS)

PLANS, FEATURES AND BENEFITS SUMMARY

Core ID Services, LLC - 2011- 2020
Confidential & Proprietary

Identity Protection Services (IPS)

PLANS AND FEATURES COMPARISON		RECOVERY	ESSENTIALS	COMPLETE
CORRECT	True Fully Managed Recovery™ Comprehensive Identity Theft restoration services provided by in-house CIPA® Certified Recovery Experts based in the U.S.A.	✓	✓	✓
	Critical Document Replacement Obtain lost or stolen ID, payment cards and critical documents on your behalf due to error, accident, theft, fire or flood.	✓	✓	✓
	Credit Report Track™ Reminders to review your free annual credit reports.	✓	✓	✓
	24x7 Support Center Access	✓	✓	✓
PROTECT	MyCoreID.com™ Portal Online and Mobile Access Secure member-only gateway to all plan benefits and information.	✓	✓	✓
	Member Newsletter & Education Resources, tips and information on identity theft and digital safety.	✓	✓	✓
	Identity Fraud Insurance Up to \$1,000,000 coverage available.		\$1,000,000	\$1,000,000
	Real-time Risk Alerts™ Email or text alerts when our monitoring detects activity.		✓	✓
	Monthly Risk Status™ A monthly snapshot of your recent monitoring results.		✓	✓
DETECT	ID CheckPoint™ (ID Verification Monitoring) Triggered by the verification process used to protect your accounts and other personal data.		✓	✓
	IDTrack™ (Identity Profile Monitoring) Monitors your full identity profile to detect fraud before it hits your credit report.			✓
	HackTrack™ (Data Breach Monitoring) Follows known data breaches to track down your stolen data.			✓
	CyberTrack™ (Dark-Web Monitoring) Searches for your data in the Internet Black Market.			✓

Additional Information:

- Family coverage – We try to keep it simple: All family members in your household that you are financially responsible for regardless of age (As always, see the definitions for additional details).

Subscription Benefits:

- Recovery support is limited to future recovery events after the original effective date for all eligible, enrolled and covered members of our RECOVERY, ESSENTIALS and COMPLETE plans.
- Pre-existing recovery event support is not included.

Group Benefits:

- Pre-existing recovery event support exclusion is waived with enrollment during a members first eligibility period.
- Plans are portable and available after separation when coverage is maintained without any break in service. Contact customer service for assistance in transitioning your plan and coverage

Plans

RECOVERY

Recovery provides our fully-managed identity theft recovery services (CORRECTION) in the event of identity fraud or theft and delivers resources to arm you with additional defenses to mitigate risks to identity, time and money.

ESSENTIALS

Essentials provides proactive identity monitoring (DETECTION), identity fraud insurance (PROTECTION), and our fully-managed identity theft recovery services (CORRECTION) in the event of identity fraud or theft and delivers resources arming you with additional defenses to mitigate risks to identity, time and money.

COMPLETE

Complete provides comprehensive identity monitoring (DETECTION), identity fraud insurance (PROTECTION), and our fully-managed identity theft recovery services (CORRECTION) in the event of identity fraud or theft and delivers resources to arm you with additional defenses to mitigate risks to identity, time and money.

Coverages

INDIVIDUAL

Plans with an INDIVIDUAL designation include that Plans' Features for the Primary Member only.

FAMILY

Plans with a FAMILY designation include that Plan's Features for the Primary Member and their eligible, enrolled and covered Family Members.

PLUS

Plans with a PLUS designation include only the RECOVERY Plan Features for the eligible, enrolled and covered Family members of the Primary Member.

ACTIVATING YOUR FULL PLAN BENEFITS

Personal Information required to enjoy the full benefits of plans with identity monitoring and insurance includes: Full Name, Physical Mailing Address, Phone Number(s), Email(s), Social Security Number and Date of Birth.

IMPORTANT NOTE

It is important to know that no company, resource or combination of resources can totally prevent identity theft or fraud from occurring. However, it doesn't mean the fight is over. When you are covered by Identity Protection Services (IPS) from Core ID Services plans our proactive monitoring, educational information and online resources complement the support of our Certified Recovery Experts (CREs) to help mitigate this growing issue for you and your family.

Table of Contents

Welcome!	2
True Fully Managed Recovery	3
Critical Document Replacement	4
MyCoreID.com Portal Access	4
Credit Report Track™	5
Member Newsletter	5
Personal Identity Monitoring and RiskAlert™ Notifications	5
RiskStatus™ and Notifications	5
ID CheckPoint™ Monitoring	6
IDTrack™ Monitoring	6
HackTrack™ Monitoring	6
CyberTrack™ Monitoring	6
Identity Theft Insurance	6
Terms & Conditions of Service	7
Identity Fraud Insurance	14



Welcome!

Identity Protection Services (IPS) from Core ID Services™ (Core ID) provides real help for identity theft, with the most comprehensive monitoring and managed recovery services possible to identity theft victims. Starting with just one phone call, we can handle all aspects of resolving identity theft, including placing fraud alerts, clearing credit reports, notifying the FTC and other necessary government agencies, replacing lost or stolen documents, alerting bank and credit institutions, and providing Identity Theft Insurance. Core ID offers a range of options for monitoring, detecting, and alerting you to identity theft in its earliest stages. We also provide our members with knowledge and insight into the newest fraud schemes, the best ways to protect against identity theft, and your own personal risk for identity theft through our member newsletter and the secure MyCoreID.com web portal. This document provides comprehensive information on all various features, so be sure to refer to your specific plan type for coverages in effect (i.e. – individual or family, levels of monitoring, insurance limits, etc.).



True Fully Managed Recovery

Core ID Services' team of in-house CIPA® Certified Recovery Experts (CREs) will work on behalf of the Covered Member(s) to restore their identity in the event of identity theft.

YOUR CRE WILL:

- Provide crisis intervention during the interview process.
- Be available for toll-free telephone access.
- Identify all known types of identity theft that have occurred.
- Send immediate notifications to banking institutions/creditors/agencies concerning the fraud.
- Provide the Covered Member with all the necessary documents (including limited power of attorney), completed and ready for signatures/notarizations, delivered via secure overnight service with overnight prepaid return envelope provided.
- Provide guidance in obtaining a police report, if needed.
- Upon return of signed documents, your CRE will process them and distribute to the appropriate agencies and organizations.
- Act on the Covered Member's behalf to fully eradicate the identity fraud from their record.
- Ensure all three credit reports are cleared of any fraudulent activity.
- Request a PIN number from the IRS to protect the Covered Member's tax refund.
- Follow through with all clearing documentation.
- Communicate fully on the status and outcome of the case, including notification when the restoration is complete.
- Send a detailed closure letter upon resolution of the Covered Member's case, stating the outcome and providing recommendations for protecting your identity in the future.

Critical Document Replacement

YOUR CRE WILL:

- Provide replacement assistance for personal documents lost, destroyed or stolen. This includes fire, flood, natural disaster, home break-in, theft or loss.
- Consult with the Covered Member to ascertain the severity of the event and to start the notification process.
- Identify missing documents.
- Contact every creditor/bank in question while the Covered Member is on the phone.
- Cancel the Covered Member's affected credit cards, licenses and other documents as needed.
- Request new replacement cards, documents, PIN numbers, etc.
- In most cases Core ID can provide completed forms necessary to obtain replacement documents.
- If the personal documents were stolen, Core ID will initiate the fraud affidavit and coordinate a police report.
- In the event of identity fraud or identity theft, Core ID will provide complete identity theft recovery for the Covered Member at no additional charge.

MyCoreID.com Portal Access

Every Covered Member can have access to our secure, personalized web portal and all the info, resources and support available with their plan.

- Profile Information and ability to add eligible family members.
- Program details, including products & services available under the subscribed plan.
- Any available upgrades can be purchased.
- Educational information including helpful tips to protect yourself.
- Archives of monthly newsletters.
- Better practices to mitigate identity theft.
- Timely updates on data breaches.
- Direct access to member help desk.

Credit Report Track™

We highly recommend our Covered Members take advantage of their federally mandated right to request their free annual credit report from each of the three credit reporting agencies. Our Credit Report Track™ reminds you on a rotating basis at four-month intervals to review your reports.

- In the event of fraudulent or potential identity theft, Core ID will begin the recovery process immediately.
- Core ID will work with the Covered Member to remove any invalid or incorrect information on their report.
- Core ID will provide assistance to Covered Members in reading and understanding credit reports.
- Core ID is NOT a credit repair service and will not provide guidance regarding financial, credit, or debt information.

Member Newsletter

Our monthly e-newsletter gives our Covered Members important information and updates about protecting their identity. Topics like child identity theft, bank fraud, tax ID theft, recent data breaches and the latest scam warnings, each issue tackles recent trends in identity theft and gives members tips and alerts that can help them avoid fraud.

Personal Identity Monitoring and RiskAlert™ Notifications

We issue real-time alerts of any activities we detect through ID CheckPoint™, IDTrack™, HackTrack™ or CyberTrack™ monitoring, sent via email or text direct to your phone. You can respond to the RiskAlert™ to indicate if the activity was legitimate (you were the one initiating the activity); or if this was a potentially fraudulent attempt. This rapid notification and response capability allow you to catch fraud early and request immediate Fully managed Recovery services through your plan. Every notification will include the company it's associated with. For additional information on the activity that triggered the RiskAlert™, you can visit your private profile page on the MyCoreID.com portal.

RiskStatus™ and Notifications

Your RiskStatus™ is a snapshot of each Covered Member's recent monitoring results in a clear, easy-to-read, color-coded graphic. Each Covered Member's RiskStatus™ is sent monthly via email and/or text direct to your phone, and available any time at MyCoreID.com. Click to drill down for details on the activity we've detected on your ID profile. RiskStatus™ will change based on the recency and frequency of monitoring alerts.

ID CheckPoint™ Monitoring

With ID CheckPoint™ Monitoring, we monitor identity verifications at banks, credit card companies and other financial service providers; mobile and other phone service providers; retailers; health insurance and medical service providers; brokerage firms; employers; money transfer services; and payday loan providers - over 300 companies in all. Suspicious or failed attempts to clear the identity verification process using any Covered Member's identity profile will trigger a RiskAlert™ notification.

IDTrack™ Monitoring

IDTrack™ Monitoring gives you inside access to the companies and systems that use, store, and possibly share the Covered Members' personal data to keep watch over your ID. Suspicious use of any covered member's identity profile, such as non-matching addresses or repeated login attempts, will trigger a RiskAlert™ notification.

HackTrack™ Monitoring

Once the Covered Member's identity, credentials or other sensitive data has been stolen in a data breach, it often changes hands many times on the black-market websites and networks that cater to identity thieves. With HackTrack™, we stay hot on hackers' heels, trolling for stolen data.

CyberTrack™ Monitoring

With CyberTrack™, we use a sophisticated bot network to crawl the Internet in addition to human resources that hack the hackers in search of any Covered Member's personal information within the Underground Economy. This proactive approach, focused on finding your compromised data, helps stop cyberthieves in action.

Identity Theft Insurance

The Identity Fraud Expense Reimbursement benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company.

Please find additional details in the sections that follow the Terms & Conditions of Service.

Terms & Conditions of Service

This End User Services Agreement (this “Agreement”) is between Core ID Services, LLC (“Core ID”) and the individual whose identity will be protected or repaired by means of the Core ID Identity Protection Services (“you”).

The person who accepts this Agreement represents and warrants to Core ID that he or she is either the individual whose identity will be protected or repaired by means of the services or is authorized by that individual to accept this Agreement on that individual’s behalf.

If the individual whose identity will be protected or repaired is under the age of eighteen (18), please see Section 12 (Identity Protection Services for Children) below.

SERVICES AGREEMENT

Core ID offers different types of identity protection and identity repair services. Some services are offered on a subscription basis and require advance enrollment or registration, and some services are offered on demand, without advance enrollment required. The features of the different services are described on the Core ID website/portal (the “Site”). The terms and conditions applicable to the enrollment-based services are stated in this Agreement.

SERVICES

Core ID may be under contract with an organization to offer the identity protection services to you because you, or a member of your family, are a customer, employee, member, end user, or other constituent of the organization. The sponsoring organization may have agreed with Core ID to pay all or part of the fees for the services offered to you. The organization may also have given Core ID your name, contact information and other information to enable Core ID to communicate with you about the offer and provide the identity protection services. If you choose to use the sponsored services, Core ID may communicate this fact to the sponsoring organization, but it will not share with the organization any personal information you provide directly to Core ID without your consent. Please see the Core ID Privacy Policy for Core ID’s commitment to protect your personal information.

ENROLLMENT/FEES

To enroll in a Core ID service, you must follow the instructions for enrollment on the Core ID Site. If you have been provided with a promotion code for a free or discounted service, you must enter the code as part of your enrollment. If you select a service that has not been fully paid on your behalf, you will be required to enter payment billing information as part of your enrollment. Depending on the service you select, you may have the option to activate certain service features by following the directions on the Site. The fee for those services are the same, whether or not you choose to activate the optional features.

SERVICE TERM

Sponsored Services – If the services provided to you have been paid for by a sponsoring organization, then the service will terminate at the end of the sponsored term, unless you elect to renew personally. Core ID will notify you prior to your sponsored services ending.

Paid Services – The initial service term begins on the date that enrollment is completed and continues for that number of months stated on the Site or in the service offer communicated to you. If you have paid for the service yourself, then the service will automatically renew at the end of the initial service term on a month-to-month basis until you contact Core ID to cancel your protection services.

CANCELLATION OF SERVICES

Direct purchase – If you purchased coverage directly through our online resources or by phone, you may cancel your subscription to any or all services at any time by calling us at (855) 262-7612 and informing us of your decision. Cancellation will be effective immediately. If you prepaid for more than one (1) month of service, you will receive a pro rata refund when you cancel. A yearly subscription requires a three (3) month minimum payment so the pro rata amount will be based on nine (9) months remaining unless the cancellation occurs within the first three (3) months at which the entire 9 months will be refunded.

Sponsored Coverage – If coverage was purchased through a sponsored benefit plan may only be cancelled through the sponsored party in writing to Core ID. Group cancellations are bound by the terms of that group coverage with Core ID.

Cancellation by Core ID – (a) Core ID may cancel services at any time upon written notice to you. On cancellation, Core ID will refund any fees you may have prepaid for the remaining unused calendar months of your service term to the payment method used to purchase the service. (b) In the event that your sponsoring organization fails to pay Core ID for your services, Core ID may cancel services at any time upon written notice to you.

UPGRADES, MULTIPLE OVERLAPPING SERVICES

If you move or upgrade to a new service, you will forfeit any remaining entitlement in your previous service. The foregoing applies only to actions taken by you in connection with your service. In the event that Core ID adds new or upgraded functionality to the products or services you currently receive, your current service entitlement will not be impacted.

AUTHORIZATION TO USE YOUR PERSONAL DATA

As part of your enrollment you will be asked to provide information that identifies you individually or that may, when combined with other information, be used to identify you individually. For example, you may be asked to provide your name, contact information (such as phone number, email, physical address), identification numbers (such as your Social Security number), account information (credit cards and related numbers), and demographic data (such as age, gender). You authorize Core ID and its subcontractors to use and share your personal data as necessary to provide you with identity repair and protection services. For example, Core ID may work with credit reporting agencies and other monitoring agencies to obtain and monitor the information they have about you. Core ID will use and protect your personal data as described in the Core ID Privacy Policy. You agree that this authorization constitutes your written instructions to obtain your credit information in accordance with the Fair Credit Reporting Act. You represent and warrant to Core ID that the information you provide describes you and not another individual and is accurate. In the event that you are registering on behalf of another adult individual, you represent and warrant to Core ID that (a) you have the express consent of all such adults that you register to submit their information to Core ID with the intent to utilize the services and to agree to this Agreement on their behalf, and (b) each adult you register for the service has read and accepted the terms and conditions of this Agreement, and he or she authorizes Core ID and its subcontractors to use and share his or her personal data as necessary to provide him or her with identity protection and repair services.

WARRANTIES & DISCLAIMER

Core ID will use commercially reasonable efforts to take those identity protection or identity repair steps described for the service you select. Otherwise the services are provided AS IS, and Core ID expressly disclaims any implied warranties, such as any implied warranty of merchantability or fitness for a particular purpose, and any warranty that may arise from a course of dealing. You acknowledge that Core ID has no obligation to take any steps not described for your service, and that those steps described for your service may not fully repair or protect your identity. You acknowledge that the Core ID services are designed to help in the event a person other than you uses or tries to use your personal data (your identity) to fraudulently obtain goods or services, and are not intended to serve any other purpose, such as credit establishment and enhancement or credit repair. Access to the Services may include hyperlinks to other web sites that are not owned or controlled by Core ID. Core ID has no control over, and assumes no responsibility for, the content, privacy policies, or practices of any third-party websites. You acknowledge and agree that Core ID is not responsible for the availability of any such external sites or resources, and does not endorse any advertising, products or other materials on or available from such web sites or resources. You acknowledge and agree that Core ID is not liable for any loss or damage which may be incurred by you as a result of the availability of those external sites or resources, or as a result of any reliance placed by you on the completeness, accuracy or existence of any advertising, products or other materials on, or available from, such web sites or resources. Core ID encourages you to read the terms and conditions and privacy policy of each other website that you visit.



LIMITATION OF CORE ID'S LIABILITY

You agree that Core ID's liability to you in connection with any legal claim you may have against it in connection with the services or this Agreement is limited as described in this Section, except to the extent these limitations are prohibited by applicable law. You acknowledge that Core ID has set its fees in reliance on your agreement to these limitations of liability. Core ID is not responsible to you for any indirect, special, incidental, punitive, or consequential loss or damage of any kind arising in connection with this Agreement or the services. The maximum liability of Core ID to you in connection with the services and this Agreement for other types of damages is a refund of fees paid by you for the services you selected. You agree that this limitation applies to any claim you might have against Core ID under any theory – contract, tort, commercial code, strict liability or otherwise, even if a limited remedy fails of its essential purpose.

SUSPENSION, TERMINATION FOR VIOLATION OF THE AGREEMENT

Either party to this Agreement (Core ID or you) may terminate this Agreement for breach if the other party is in material violation of this Agreement and fails to cure the violation within ten (10) days of the party's written notice describing the breach in reasonable detail, or if the other party provides or uses the services (as applicable) in violation of applicable law. In addition, Core ID may suspend performance of the services if you have failed to timely pay the fees for the services or are otherwise in breach of the Agreement. If Core ID suspends the services under this Section, it will reinstate the services when you have remedied the violation, unless it terminates the agreement prior to that time. If suspension is due to late payment, Core ID may require you to prepay the fees for the entire subscription as a condition to reinstating the services. If Core ID terminates the Agreement for your breach, it is not obligated to refund any fees you may have prepaid for the services.

CONFIDENTIAL AND PROPRIETARY INFORMATION

Core ID's services techniques, processes, fees, and client- or subscriber-related information are confidential or proprietary information. You may not use or disclose that information for any purpose other than as necessary to use the Core ID services for the repair or protection of your identity. If you give Core ID feedback on its services, you license the feedback and any related intellectual property to Core ID on a perpetual, non-exclusive, irrevocable, fully paid basis, to use, modify, distribute, and commercially exploit without restriction or obligation to account to you. Except as expressly stated otherwise in this Agreement, each party retains all right, title and interest in and to its intellectual property. You may not reverse engineer, decompile, disassemble or take like action with respect to the services or any Core ID technology except to the extent such activity is permitted by applicable law notwithstanding this limitation, and then only on advance written notice to Core ID of at least thirty (30) days.

IDENTITY PROTECTION SERVICES FOR CHILDREN

Notwithstanding anything to the contrary above, if the individual whose identity is to be protected or repaired by means of the services is under the age of eighteen (18) (a “Child”), then the person who enrolls the Child represents and warrants that he or she is the individual’s parent or guardian with authority to enroll the Child and provide the Child’s personally identifiable data. The references to “you” in this Agreement should be interpreted to refer to the Child or the authorized parent or guardian, as appropriate to the context.

GOVERNING LAW

This Agreement is governed by the laws of the State of Georgia and the United States of America, as applicable, excluding any law that would require the laws of a different jurisdiction be applied.

DISPUTES

The following dispute resolution process applies solely to disputes which may arise between you and Core ID and does not interfere with your ability to bring class, collective, or other legal actions against the sponsor organization or any other party. Each party to this Agreement (you and Core ID) agree that any dispute related to the Services or this Agreement shall be submitted to binding arbitration in Atlanta, Georgia. The arbitration shall be conducted by one arbitrator in accordance with the commercial arbitration rules of the American Arbitration Association (“AAA”). The arbitration will be conducted in person unless each of us agrees to a telephonic or written submissions procedure. The arbitrator shall issue a reasoned award with findings of fact and conclusions of law and judgment on the award rendered by the arbitrator may be entered in any court having jurisdiction. Either party may bring an action in any court of competent jurisdiction to compel arbitration under this Agreement, or to enforce or vacate an arbitration award. You waive any right to a trial by jury and agree that disputes will be resolved through arbitration. No claim subject to this provision may be brought as a class or collective action, nor may you assert such a claim as a member of a class or collective action that is brought by another claimant. Each party agrees not to bring a claim related to the Services or this Agreement more than two years after the time that the claim accrued. Except as may be required by law, neither a party nor an arbitrator may disclose the existence, content, or results of any arbitration hereunder without the prior written consent of both parties.

MISCELLANEOUS

You agree that Core ID may use your address entered as part of our enrollment for the purposes of any legal or other notices that it is required or permitted to give you in connection with the services or this Agreement. Core ID may assign this Agreement and may use subcontractors to perform its obligations under this Agreement. Core ID is responsible to you for the actions of its subcontractors to the same extent as if those actions were by Core ID. Core ID is excused from any delay in providing the services to the extent the delay is reasonable due to any event beyond its control, such as a general failure of telecommunications networks, acts of God, or other “force majeure” events. The Section captions in this Agreement are for convenience only; they are not part of this Agreement and may not be used to interpret the terms of this Agreement. Nouns stated in the singular shall imply the plural as indicated by the context, and pronouns that are gender specific shall be read to refer to either gender. In the event one or more of the terms of this Agreement are adjudicated invalid, illegal, or unenforceable, the adjudicating body may either interpret this Agreement as if such terms had not been included, or may reform such terms to the limited extent necessary to make them valid, legal or enforceable, consistent with the economic and legal incentives underlying the Agreement.

ENTIRE AGREEMENT

This Agreement is the complete and exclusive agreement between the parties regarding its subject matter and supersedes and replaces in its entirety any prior or contemporaneous agreement or understanding regarding the subject matter of this Agreement, written or oral. Core ID may change this Agreement as necessary, and when we do will post the Last Updated date on this Site so you will always be aware when changes are made. In the event that a change or update is material to how you access or use the service, Core ID will make reasonable efforts to contact you regarding the change or update. Your continued use of the service will be considered acceptance of the modified terms.

Identity Fraud Insurance

Identity theft insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under a group policy issued to InfoArmor for the benefit of its (or its affiliates such as Core ID Services) Members.

The description herein on the following pages is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies presented. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



TERMS AND CONDITIONS

Summary of Benefit

These Terms and Conditions are provided to inform you that as a customer of Core ID Services or its affiliates who are enrolled in a Core ID Services Identity Protection Services membership program powered by InfoArmor that includes identity theft insurance, you are entitled to benefits under the Policy as issued to InfoArmor for use by its members and program provider Core ID Services members. The benefits are described in these Terms and Conditions. Various provisions in these Terms and Conditions and in the Policy restrict coverage. Read the entire Terms and Conditions carefully to determine rights, duties and what is and is not covered.

These Terms and Conditions do not state all the terms, conditions, exclusions and definitions within the InfoArmor Policy. Your benefits will be subject to all the terms, conditions, exclusions and definitions of the Policy as issued to InfoArmor. A complete copy of the Policy will be available upon request. If the Policy issued to InfoArmor is terminated, your benefits under the Policy will cease effective that date. It is the obligation of InfoArmor through Core ID Services to inform you of any termination of the Policy.

The Identity Fraud Expense Reimbursement benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under a group policy issued to InfoArmor for the benefit of its or its affiliates Members. To obtain a complete copy of the Policy as issued to InfoArmor, contact Core ID Services at 1 (855) 262-7612. American Bankers Insurance Company of Florida administers all claims and neither InfoArmor nor Core ID Services shall have responsibility to Members with respect to the Identity Fraud Expense Reimbursement benefit.

All references to **We**, **Us**, and **Our** throughout this Summary of Benefit means American Bankers Insurance Company of Florida.

Limits of Insurance

Coverage	Limit of Liability
Essentials or Complete	
Expense Reimbursement	\$1,000,000 Aggregate Limit per Member per 12 Month Period
Cash Recovery Aggregate	\$1,000,000 (Part of and not in addition to Expense Reimbursement Aggregate Limit of Liability)
Investment & Health Savings Accounts Cash Recovery	\$50,000 Sublimit per Member per 12 Month Period. Such Sublimit is part of the \$1,000,000 Aggregate Limit per Member per 12 Month Period

DUTIES WHEN LOSS OCCURS

Upon knowledge or discovery of loss or of an occurrence which may give rise to a claim under the terms of this coverage, the policyholder is responsible for notifying the member of the following requirements:

- a.** Give notice as soon as practicable to:
 - i. the appropriate authority and affected institutions, if applicable; and
 - ii. call 1 (855) 262-7612 to make a valid claim within sixty (60) days of the date of discovery, or as soon as reasonably possible.

If the loss involves a violation of law, the member shall also notify the police. The member must submit a copy of the police report when filing a claim;

For both Checking & Savings Account Cash Recovery and Investment and HSA Cash Recovery claims, the member must provide documentation from the financial institution that the funds were fraudulently removed and are non-recoverable from the financial institution.

- b.** File detailed proof of loss, duly sworn to, with us within sixty (60) days after the discovery of loss;
- c.** Take all reasonable steps to mitigate loss resulting from identity fraud including, but not limited to, requesting a waiver for any applicable fees, loan application fees or credit bureau fees;
- d.** Upon our request, submit to examination by us, and subscribe the same, under oath if required;
- e.** Upon our request, cooperate to help us enforce legal rights against anyone who may be liable to the member to include giving evidence and attending depositions, hearing and trials;
- f.** Immediately forward to us any notices, summons or legal papers received by the member in connection with the loss or the identity fraud;
- g.** Produce for our examination all pertinent records;
- h.** Cooperate with us in all matters pertaining to loss or claims;
all at such reasonable times and places as we shall designate.

The member shall not voluntarily assume or admit any liability, nor, except at said member's own cost, voluntarily make any payment or incur any expense without our prior written consent, such consent not to be unreasonably withheld.

The member shall keep books, receipts, bills and other records in such manner that we can accurately determine the amount of any loss. At any time, subsequent to the reporting of the loss to us, we may examine and audit the member's books and records as they relate to a loss under the Policy.

IDENTITY FRAUD – EXPENSE REIMBURSEMENT

We will reimburse the member for expenses and legal costs incurred by the member, up to the Aggregate Limit of Liability as shown on the Limits of Insurance section of these Terms and Conditions from the direct result of the following:

1. Fraud or Embezzlement

For loss arising out of fraud or embezzlement perpetrated against the member, with an occurrence date during the term of the membership.

2. Theft

For loss resulting directly from theft of property related to the member's information, checkbook, savings record, ATM access or securities from the member, with an occurrence date during the term of the membership, by a person from whom the member purchased goods or services.

3. Forgery

For loss, with an occurrence date during the term of the membership, resulting directly from forgery or alteration of checks, drafts, promissory notes, or similar written promises, orders or directions to pay money that are:

- i. Made or drawn by or drawn upon the member's account; or
- ii. Made or drawn by one purporting to act as the member's agent.

4. Data Breach

For loss, with an occurrence date during the term of the membership, resulting directly from the misuse of the member's information as a result of a data compromise of information from a financial institution, a credit reporting agency, a credit grantor, a securities firm, employer or other institution/company maintaining the member's personal information, that results in monies stolen from the member's accounts or misuse of data to obtain property, credit or monies using the member's information.

5. Stolen Identity Event

For loss resulting from a stolen identity event, including but not limited to a stolen identity event occurring on or arising out of the use of the Internet. The occurrence date must be during the term of the membership. A stolen identity event means the theft, unauthorized, or illegal use of the member's name, social security number, or other method of identifying the member.

Cash Recovery Aggregate

We will reimburse the member, up to the Aggregate Limit of Liability as shown on the Limits of Insurance section of these Terms and Conditions, a Cash Recovery Aggregate benefit limited to payment for one (1) occurrence within any twelve (12) consecutive months of the term of the membership, for recovery of traditional credit cards, pre-paid credit cards and debit card deductibles or in the event of an unauthorized electronic fund transfer, reimbursement for unrecoverable funds, exclusive of interest, directly drawn from or removed through an unauthorized electronic fund transfer from the member's mobile device (smart phone) or other financial account due to an act of fraud, embezzlement, theft, forgery or other data breach which have not been recovered.

Cash Recovery Aggregate does not cover unrecoverable funds for which the member did not seek reimbursement from the financial institution, or other provider which issued the access device and holds the account from which funds were stolen, and for which the member has not received reimbursement from any other source.

The member will only be covered from an unauthorized removal of funds or an unauthorized electronic fund transfer if the loss first occurs on or after the effective date of the Policy under which this coverage is provided, while the member is an active and paid member of the policyholder, and the loss is reported to us within ninety (90) days of discovery.

The member is not covered if the unauthorized removal of funds or unauthorized electronic fund transfer first occurs after the termination of the Policy under which this coverage is provided, or the member is not an active and paid member of the policyholder.

The Cash Recovery Aggregate benefit is part of, and not in addition to the Expense Reimbursement Aggregate Limit of Liability. We will pay up to the Aggregate Limit of Liability as shown on the Limits of Insurance section of these Terms and Conditions.

Investment & Health Savings Accounts Cash Recovery

We will reimburse the member, up to the Aggregate Limit of Liability as shown on the Limits of Insurance section of these Terms and Conditions, an Investment & Health Savings Accounts Cash Recovery benefit limited to payment for one (1) occurrence within any twelve (12) consecutive months of the term of the membership, for unrecoverable funds, exclusive of interest, removed through an unauthorized electronic fund transfer from the member's investment or health savings account, due to an act of fraud, embezzlement, theft, forgery or other data breach, which have not been recovered.

Investment & Health Savings Accounts Cash Recovery does not cover unrecoverable funds for which the member did not seek reimbursement from the financial institution, or other provider which issued the access device and holds the investment or health savings account from which funds were stolen, and for which the member has not received reimbursement from any other source.

The member will only be covered from an unauthorized electronic fund transfer if the loss first occurs on or after the effective date of this Policy under which this coverage is provided, while the member is an active and paid member of the policyholder, and the loss is reported to us within ninety (90) days of discovery.

The member is not covered if the unauthorized electronic fund transfer first occurs after the termination of the Policy under which this coverage is provided, or the member is not an active and paid member of the policyholder.

For Family Plans, the Investment & Health Savings Accounts Cash Recovery benefit is limited to payment for one (1) occurrence within twelve (12) consecutive months of the term of the Policy, not to exceed the limit of liability shown on the Declarations Page.

The Investment & Health Savings Accounts Cash Recovery benefit is part of, and not in addition to the Expense Reimbursement Aggregate Limit of Liability. For Investment & Health Savings Accounts Cash Recovery we will pay up to the Limit of Liability as shown on the Limits of Insurance section of these Terms and Conditions.

An unauthorized electronic fund transfer does not include an electronic fund transfer initiated:

1. by a person who was furnished the access device to the member's account, unless the member had given prior notification to the financial institution that transfers by such person(s) are no longer authorized;
2. with fraudulent intent by the member or any person acting in concert with the member;
3. by the financial institution or its employees; or
4. from any business or commercial account.

EXCLUSIONS

Expense Reimbursement, Cash Recovery Aggregate and Investment & Health Savings Accounts Cash Recover does not cover:

- a.** loss due to any fraudulent, dishonest or criminal act by the member or any person acting in concert with the member, or immediate family member, whether acting alone or in collusion with others;
- b.** loss resulting directly or indirectly from any errors or omissions occurring in the following actions:
 - i. the input of data to any computer system; or
 - ii. the processing of data by any computer system; or
 - iii. the manual or electronic processing of any output produced by any computer system;
- c.** loss resulting directly or indirectly from the voluntary surrendering by the member of any access device, in whole or in part, to any person or entity;
- d.** loss resulting from any unintentional clerical error in the transfer from or debit of any account of the member which is initiated by a financial institution, or any employee(s) thereof. However, this exclusion shall not apply to a fraudulent act of an employee(s) of a financial institution where said employee(s) is acting without the permission or instruction of their employer;
- e.** loss in connection with any pre-authorized transfer from any account to or for the benefit of a financial institution, or to any other account of the member;
- f.** indirect or consequential loss of any nature;
- g.** loss of potential income not realized by the member;
- h.** loss resulting from an identity fraud that was discovered prior to the effective date of the Policy under which this coverage is provided;
- i.** loss arising out of business pursuits of the member;
- j.** loss of valuable papers, valuable documents, jewelry, silverware and other personal property including the philatelic value of stamps and the numismatic value of coins not in circulation;
- k.** property damage, bodily injury or personal injury;
- l.** losses incurred from financial performance of any investment of financial product;
- m.** loss from games of chance;
- n.** for Cash Recovery Aggregate losses other than traditional credit cards, pre-paid credit cards and debit card deductibles or unrecoverable funds, exclusive of interest, directly drawn from or removed through an unauthorized electronic fund transfer from the member's mobile device (smart phone), or other financial account. , and for Investment & Health Savings Accounts Cash Recovery losses other unrecoverable funds, exclusive of interest, removed through an unauthorized electronic fund transfer from the member's investment or health savings account. All other monetary devices are excluded;
- o.** any loss, claims or damages that are not covered under the terms and provisions of the Policy under which this coverage is provided;
- p.** legal fees in excess of \$125 per hour;
- q.** any loss which occurred while the member was not an active and paid member of the policyholder.

INVESTMENT & HEALTH SAVINGS ACCOUNT CASH RECOVERY DOES NOT COVER:

- a. unauthorized electronic fund transfers from investment & health savings accounts for which the member activates online access, and a two-factor authentication, knowledge-based authentication (KBA) or other authentication process is provided by the financial institution or the HSA Custodian/Administrator and it has not been activated by the member, or authentication is not required by the financial institution or the HSA Custodian/Administrator.
- b. unauthorized electronic fund transfers resulting from the financial institution's or the HSA Custodian/Administrator's, and/or the member's failure to comply with standard or customary transfer instruction verification and approval processes and procedures, including verification and approval by the financial institution, or the HSA Custodian/Administrator, and/or the member on subsequent changes to transfer instructions.
- c. This policy does not cover loss resulting from unauthorized electronic transfers of digital currency or cryptocurrency such as Bitcoin, Ethereum, or Litecoin, or any currency not regulated or supervised by a government agency.

The member must provide documentation from the financial institution that the funds were fraudulently removed and are non-recoverable from the financial institution.

The member will only be covered from an unauthorized removal of funds or an unauthorized electronic fund transfer if the loss first occurs on or after the effective date of the Policy under which this coverage is provided, while the member is an active and paid member of the policyholder, and the loss is reported to us within ninety (90) days of discovery.

The member is not covered if the unauthorized removal of funds or unauthorized electronic fund transfer first occurs after the termination of the Policy under which this coverage is provided, or the member is not an active and paid member of the policyholder.

DEFINITIONS

Access Device means a card (including credit, debit and ATM cards), code, PIN, password, personal check or other similar means of access to the member's account at a financial institution that may be used by the member to gain access to said account for the purpose of withdrawing or transferring funds, making purchases, or making long distance or cellular/digital (wireless) telephone calls.

Account means a cash, credit card, demand deposit (checking), savings, or money market account of the association members held directly or indirectly by a financial institution and established primary for personal, family or household purposes.

Data Breach means the misuse of the member's information as a result of a data compromise of information from a financial institution, a credit reporting agency, a credit grantor, a securities firm, employer or other institution/company maintaining the member's personal information, that results in monies stolen from the member's accounts or misuse of data to obtain credit or monies using the member's information.

Date of Discovery occurs when the member first becomes aware of facts which would cause a reasonable person to assume that a loss covered by this insurance has been or will be incurred, even though the exact amount or details of loss may not then be known. Discovery also occurs when the member receives notice of an actual or potential claim against the member involving loss covered under this insurance.

Domestic Partner means a person designated in writing by the primary member who is registered as a domestic partner or legal equivalent under laws of the governing jurisdiction or who:

1. is at least 18 years of age and competent to enter into a contract;
2. is not related to the primary member by blood;
3. has exclusively lived with the primary member for at least twelve (12) consecutive months prior to the effective date of coverage;
4. is not legally married or separated; and
5. as of the date of coverage, has with the primary member at least two (2) of the following financial arrangements:
 - i. a joint mortgage or lease;
 - ii. a joint bank account;
 - iii. joint title or ownership of a home, motor vehicle or status as joint lessee on a motor vehicle lease;
 - iv. a joint credit card account with a financial institution.

Expenses mean:

1. Costs incurred by the member for re-filing applications for loans, grants, or other credit that are rejected solely because the lender received from any source incorrect information as a result of the identity fraud;
2. Costs for notarizing affidavits or other similar documents, long distance telephone calls, travel and postage reasonably incurred as a result of the member's efforts to report an identity fraud or amend or rectify records as to the member's true name or identity as a result of an identity fraud;
3. Reasonable costs incurred by the member for up to six (6) credit reports from established credit bureaus (with no more than two (2) reports from any one credit bureau) dated within twelve (12) months after the member's discovery of an identity fraud, and costs incurred for contesting the accuracy or completeness of any information contained in a credit report following an identity fraud;
4. Payment for reasonable expenses incurred for the placement of up to twelve (12) credit freezes or credit thaws per 12 month period as a result of being notified of a data breach in which the member's personal information was compromised and payment for expenses that were a result of recovery from an identity fraud such as; credit freeze, credit thaw costs, transcript costs, appeal bond, court filing fees, expert witness or courier fees;
5. Actual lost base wages that would have been earned, for time reasonably and necessarily taken off work solely as a result of efforts to amend or rectify records as to the member's true name or identity as a result of an identity fraud. Actual lost wages includes remuneration for vacation days, discretionary days, floating holidays, and paid personal days and excludes sick days, business interruption and future earnings of a self-employed professional. Coverage is limited to base wages within twelve (12) months after discovery of an identity fraud. Base wages must be supported by and based on the prior year tax return.
6. Child or elderly care costs that would have otherwise not been incurred, resulting from time reasonably and necessarily taken away from providing such care as a result of efforts to amend or rectify records as to the member's identity as a result of an identity fraud.
7. Reasonable and necessary costs incurred by the member for ordering medical records for the purpose of amending and/or rectifying these documents as a result of an identity fraud.
8. Reasonable and necessary costs incurred by member for the replacement of identification cards, driver licenses and passports as a result of an identity fraud.
9. Reasonable and necessary costs, up to a maximum of \$125 per hour, incurred by the member for use of any investigative agency or private investigator engaged to amend or rectify records as to the member's true name or identity as a result of an identity fraud. We reserve the right to select such investigative agency or private investigator; however, with our express prior written consent, member may elect such investigative agency or private investigator.
10. Reasonable and necessary costs, up to a maximum of \$125 per hour, incurred by the member associated with the use of any certified public accountant engaged to amend or rectify records as to the member's true name or identity as a result of an identity fraud. We reserve the right to select such certified public accountant; however, with our express prior written consent, member may elect such certified public accountant.

Family Member means the primary member's spouse or domestic partner, parent, siblings, children and/or any other member of, or dependent persons residing in the primary member's household. Family member also includes a primary member's spouse or domestic partner's:

1. unmarried children (including those who the member is their legal guardian) under twenty-one (21) years of age.
2. unmarried children (including those who the member is a legal guardian) under twenty-six (26) years of age if a full-time student at an accredited college or university.
3. dependent(s) with documented disabilities who have the same primary residence as the member and who relies on the member for maintenance and support.

Any family member who does not reside at the primary member's home is not eligible for coverage, except unmarried children (including those who the member is a legal guardian) under twenty-six (26) years of age if a full-time student at an accredited college or university.

The Aggregate Limit of Liability shown on the on the Limits of Insurance section of these Terms and Conditions will be the maximum amount we will pay for all covered losses per Member regardless of the number of losses that occur for any member per twelve (12) month period.

Forgery means the signing of the name of another person or organization with intent to deceive. It does not mean a signature, which consists in whole or in part of one's own name signed, in any capacity, for any purpose.

Fraud or Embezzlement includes electronic, telegraphic cable, teletype tele facsimile, telephone or written instructions which: purports to have been transmitted or written by the member, but which was in fact fraudulently transmitted or altered by someone else without member's knowledge or consent; or received by the member which purports to have been transmitted by an employee but which was in fact fraudulently transmitted by someone else without member's or employee's knowledge or consent.

HSA Custodian/Administrator means a bank, credit union, insurance company, brokerage or other IRS-approved organization that offers health savings accounts.

Identity Fraud means the act of knowingly transferring or using, without lawful authority, a means of identification of the member with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal, State or local law.

Investment or Health Savings Accounts means an employee sponsored, retirement or health savings account such as a 401K, Roth 401K, Simple IRA, SEP IRA, Health Savings Account (HSA), Flexible Spending Account (FSA), or Health Reimbursement Account (HRA). Investment or Health Savings Accounts also includes Employee Stock Option Plans (ESOP) of the member held directly or indirectly by a financial institution or HSACustodian/Administrator and established primarily for personal, family or household purposes.

Legal Costs means costs, up to a maximum of \$125 per hour, for reasonable fees for an attorney fees for an attorney selected by the member and related court fees, incurred by the member with our consent, for:

1. Defense of any legal action brought against the member by a merchant, creditor or collection agency or entity acting on their behalf for non-payment of goods or services or default on a loan as a result of the identity fraud;
2. Defense of or the removal of any civil judgments wrongly entered against the member as a result of identity fraud; and
3. Challenging the accuracy or completeness of any information in a member's consumer credit report, medical history or tax history, as a result of identity fraud; and
4. Member's initial consultation with a lawyer to determine the severity of and appropriate response to an identity fraud.

Loss means the expenses and legal costs incurred by the member as the direct result of a covered transaction.

Member means the primary member and primary member's family member if the primary member is enrolled in or elects a Family Plan membership program.

Occurrence means an incident of an actual or attempted fraudulent, dishonest or criminal act or series of related acts, whether committed by one or more persons.

Occurrence date means the earliest possible date of discovery.

Policyholder means InfoArmor, a member company of Allstate.

Primary Member means a customer of Core ID Services or its affiliates who is enrolled in a Core ID Services Identity Protection Services membership program powered by InfoArmor that includes identity theft insurance who is in good standing:

1. for which the primary member membership fee/ product fee has been paid; and
2. whose name is shown on the membership.

Proof of Loss means receipts for reasonable out of pocket expenses.

Spouse means a person who is either:

1. legally married to the primary member; or
2. meets the definition of domestic partner to the primary member.

Stolen Identity Event means the theft, unauthorized, or illegal use of the member's name, social security number, or other method of identifying the member.

Unauthorized Electronic Fund Transfer (UEFT) means an electronic fund transfer from the member's account for Cash Recovery Aggregate, or investment or health savings account for Investment & Health Savings Accounts Cash Recovery, initiated by a person other than the member without the actual authority to initiate such transfer and from which the member receives no benefit.

An unauthorized electronic fund transfer does not include an electronic fund transfer initiated:

1. by a person who was furnished the access device to the member's account, unless the member had given prior notification to the financial institution that transfers by such person(s) are no longer authorized;
2. with fraudulent intent by the member or any person acting in concert with the member;
3. by the financial institution or its employees; or
4. from any business or commercial account.

Conditions

1. Limits of Insurance

Our maximum limit of liability for loss under these Terms and Conditions shall not exceed the applicable limit stated on the Limits of Insurance section of these Terms and Conditions.

All loss incidental to an actual or attempted fraudulent, dishonest or criminal act or series of related acts, whether committed by one or more persons, shall be deemed to arise out of one occurrence.

Our total aggregate limit of liability shown on the Limits of Insurance section of these Terms and Conditions will be the maximum amount we will pay for all covered losses per member, regardless of the number of losses that occur for that member per twelve (12) month period.

2. Loss Payment

We will pay any loss covered under the Policy under which this coverage is provided, within thirty (30) days after:

- a. We reach agreement with the member; or
- b. The entry of final judgment.

3. Notice of Claim must be given to us by the member:

- a. in writing; and
- b. within a reasonable time period after the date of discovery.

4. Settlement of Claims

We will pay all covered claims within ninety (90) days from the date we receive acceptable proof of loss at our office.

5. Transfer of Rights of Recovery Against Others to Us

If any person or organization to or for whom we make payment under this insurance has rights to recover damages from another, those rights are transferred to That person or organization must do everything necessary to secure our rights and must do nothing to impair them.

Recovery against persons or organizations also insured under this Policy or any other Policy issued by us with respect to the same loss is prohibited.

6. Other Insurance

This insurance is excess in the event coverage is provided under any other policy/certificate.

Should member be enrolled in more than one membership program insured by us, we will reimburse the member under each membership:

- a. subject to the applicable deductibles and limits of liability of each membership;
- b. but in no event shall the total amount reimbursed under all memberships exceed the actual amount of loss; and
- c. in no event shall the limit of liability under all memberships exceed the largest limit of liability available to the member under any membership program insured by us.

7. Action Against Us

No action may be brought against us unless there has been full compliance with all of the terms and conditions of this Summary of Benefits and suit is filed within twenty-four (24) months from the date of occurrence. No one will have the right to join us as a party to any against the policyholder or member.



CORE ID

S E R V I C E S

Core ID Services, LLC
2425 Commerce Ave NW
Suite 300
Duluth, GA 30096

855-262-7612 | customerservice@coreidservices.com | coreidservices.com

