Goodwin Procter LLP
The New York Times Building
620 Eighth Avenue
New York, NY 10018

goodwinlaw.com

Confidential Treatment Requested

December 19, 2025

VIA PORTAL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

RE: Notice of Data Event

Dear Sir or Madam:

We represent OutdoorSmart! Inc., which operates the Campfire Collective website, and are writing to notify your Office, pursuant to RCW § 19.255, of a compromise that affected the security of certain personal information relating to 652 Washington residents. By providing this notice, Outdoor Smart does not waive any rights or defenses, including but not limited to rights or defenses regarding the applicability of Washington law, the applicability of Washington data event notification statute, or personal jurisdiction.

Notice of Data Event

On November 3, 2025, OutdoorSmart was alerted by its payment processing partner to unusual activity that the partner believed may have originated from the Campfire Collective website. OutdoorSmart promptly initiated its incident response protocols. After an investigation, with the assistance of third-party cybersecurity specialists, Outdoor Smart identified the presence of unauthorized code capable of capturing payment card information used when making purchases on the Campfire Collective website. The unauthorized capturing of payment card information may have occurred between February 15, 2024 and November 4, 2025. Outdoor Smart immediately removed the unauthorized code on November 4, 2025.

Outdoor Smart has investigated this matter with the assistance of third party specialists and confirmed that the unauthorized code is no longer present. On December 4, 2025, Outdoor Smart confirmed that certain personal information might have been impacted in a recent security incident.

Following this discovery, OutdoorSmart moved quickly to contain and remediate the Incident, an effort which has since completed. As part of its ongoing commitment to information security, we are reviewing our existing policies and procedures. In addition, OutdoorSmart is undertaking additional security related measures to enhances its cybersecurity posture.

The personal information involved may include name, and payment card information, including card type, card number, expiration date and CVC.

Notice to Washington Residents

On December 19, 2025, OutdoorSmart began providing written notice of the Incident to potentially impacted individuals which includes Washington residents. Written notice is being provided in substantially the same form as the letter attached hereto as *Exhibit A*. The notification letter includes complimentary access to credit monitoring and identity restoration services for twenty-four (24) months through Epiq.

Other Steps Taken and to be Taken

Upon discovery of the Incident, OutdoorSmart moved quickly to investigate and respond to the Incident, assess the security of its systems, and notify potentially impacted individuals. OutdoorSmart also reviewed its existing policies and procedures and implemented additional safeguards to further secure its systems and the information contained therein.

OutdoorSmart is offering potentially impacted individuals with access to complimentary credit monitoring for twenty-four (24) months and dedicated call center services as well as providing guidance on how to protect against identity theft and fraud, including advising individuals to report any suspected identity theft or fraud to their financial institutions. OutdoorSmart is also providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national credit reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for fraud and identity theft by reviewing account statements and monitoring credit reports, and encouragement to contact the Federal Trade Commission, their Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the Incident, please contact me at cyber@goodwinlaw.com.

Respectfully submitted,

Goodwin Procter LLP

/s/ *Kaitlin Betancourt*

Kaitlin Betancourt
Partner

KB

EXHIBIT A

(SEE ATTACHED)

OUTDOORsmart!

Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

<<VARIABLE DATA 1>>

Dear <<Full Name>>:

OutdoorSmart! Inc., which operates the Campfire Collective website, is writing to advise you of a recent event that may impact the security of certain personal information related to you. We write to provide you with information about the incident, the steps we have taken since discovering the incident, and the steps you can take to better protect your information should you feel it appropriate to do so.

What Happened? On November 3, 2025, Outdoor Smart was alerted to unusual activity on its Campfire Collective website and promptly initiated its incident response protocols. After an investigation, with the assistance of third-party cybersecurity specialists, Outdoor Smart identified the presence of unauthorized code capable of capturing payment card information used when making purchases on the Campfire Collective website. The unauthorized capturing of payment card information may have occurred between February 15, 2024 and November 4, 2025. Outdoor Smart immediately removed the unauthorized code on November 4, 2025.

Outdoor Smart has investigated this matter with the assistance of third party specialists and confirmed that the unauthorized code is no longer present. On December 4, 2025, Outdoor Smart confirmed that certain of your information might have been impacted in a recent security incident.

What Information Was Involved? The personal information involved may include your name, and payment card information, including card type <<Variable Data 2>>, card number, expiration date and CVC.

What We Are Doing. We take this event and the security of personal information in our care seriously. We moved quickly to respond and mitigate the issue and notify individuals. As part of our ongoing commitment to information security, we are reviewing our existing policies and procedures. As an added precaution, we are providing you with 24 months of complimentary access to credit monitoring and identity restoration services through Epiq as well as guidance on how to better protect your information. Enrollment information is contained in the attached *Steps You Can Take to Protect Personal Information***.** We are unable to enroll you in these services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Protect Personal Information*. There, you will find more information on the credit monitoring and identity restoration services we are making available to you. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have questions you may contact our dedicated assistance line at 888-367-0556, Monday through Friday from 9:00 am ET to 9:00 pm ET, excluding major U.S. holidays. You may also write to Outdoor Smart at Unit 2, 890 Taylor Creek Drive, Ottawa, Ontario K4A 0Z9.

Sincerely,

OutdoorSmart! Inc

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

<<Full Name>>
Activation Code: <<ACTIVATION CODE>>
Enrollment Deadline: <<ENROLLMENT DEADLINE>>
Coverage Length: 24 Months

Epiq - Privacy Solutions ID
3B Credit Monitoring

How To Enroll:

1) Visit www.privacysolutionsid.com and click "Activate Account"
2) Enter the following activation code, **<<Activation Code>>** and complete the enrollment form
3) Complete the identity verification process
4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
5) Enter your log-in credentials
6) You will be directed to your dashboard and activation is complete!

Product Features:

3-Bureau Credit Monitoring with Alerts
Monitors your credit file(s) with each of the 3 Credit Bureaus for key changes, with alerts such as credit inquiries, new accounts, and public records.

VantageScore® 3.0 Credit Score with Score Tracker[1]
1-Bureau VantageScore®3.0 (monthly) and Credit Score Tracker.

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)
Detect and prevent common identity theft events outside of what is on your credit report. Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, online document signings and payment platforms, with alerts.

Dark Web Monitoring
Scans millions of servers, online chat rooms, message boards, and websites across all sides of the web to detect fraudulent use of your personal information, with alerts.

Change of Address Monitoring
Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users' current or past addresses.

Credit Protection
3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Personal Info Protection
Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers – so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

Identity Restoration & Lost Wallet Assistance
Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

Up to $1M Identity Theft Insurance[2]
Provides up to $1,000,000 ($0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer- UEFT[2]
Provides up to $1,000,000 ($0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity (occurrence based).

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 3B Credit Monitoring, please call directly at **866.675.2006**, Monday-Friday 9:00 a.m. to 5:30 p.m., ET.

1 The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore® credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

2 Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. or American Bankers Insurance Company of Florida, an Assurant company. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

*For Iowa Residents***:** Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut St., Des Moines, IA 50319, Telephone: 515-281-5164, www.iowaattorneygeneral.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately <<Rhode Island Count>> Rhode Island residents that may be impacted by this event.

Goodwin Procter LLP
The New York Times Building
620 Eighth Avenue
New York, NY 10018

goodwinlaw.com

Confidential Treatment Requested

December 19, 2025

VIA PORTAL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

RE: Notice of Data Event

Dear Sir or Madam:

We represent OutdoorSmart! Inc., which operates the Campfire Collective website, and are writing to notify your Office, pursuant to RCW § 19.255, of a compromise that affected the security of certain personal information relating to 652 Washington residents. By providing this notice, Outdoor Smart does not waive any rights or defenses, including but not limited to rights or defenses regarding the applicability of Washington law, the applicability of Washington data event notification statute, or personal jurisdiction.

Notice of Data Event

On November 3, 2025, OutdoorSmart was alerted by its payment processing partner to unusual activity that the partner believed may have originated from the Campfire Collective website. OutdoorSmart promptly initiated its incident response protocols. After an investigation, with the assistance of third-party cybersecurity specialists, Outdoor Smart identified the presence of unauthorized code capable of capturing payment card information used when making purchases on the Campfire Collective website. The unauthorized capturing of payment card information may have occurred between February 15, 2024 and November 4, 2025. Outdoor Smart immediately removed the unauthorized code on November 4, 2025.

Outdoor Smart has investigated this matter with the assistance of third party specialists and confirmed that the unauthorized code is no longer present. On December 4, 2025, Outdoor Smart confirmed that certain personal information might have been impacted in a recent security incident.

Following this discovery, OutdoorSmart moved quickly to contain and remediate the Incident, an effort which has since completed. As part of its ongoing commitment to information security, we are reviewing our existing policies and procedures. In addition, OutdoorSmart is undertaking additional security related measures to enhances its cybersecurity posture.

The personal information involved may include name, and payment card information, including card type, card number, expiration date and CVC.

Notice to Washington Residents

On December 19, 2025, OutdoorSmart began providing written notice of the Incident to potentially impacted individuals which includes Washington residents. Written notice is being provided in substantially the same form as the letter attached hereto as *Exhibit A*. The notification letter includes complimentary access to credit monitoring and identity restoration services for twenty-four (24) months through Epiq.

Other Steps Taken and to be Taken

Upon discovery of the Incident, OutdoorSmart moved quickly to investigate and respond to the Incident, assess the security of its systems, and notify potentially impacted individuals. OutdoorSmart also reviewed its existing policies and procedures and implemented additional safeguards to further secure its systems and the information contained therein.

OutdoorSmart is offering potentially impacted individuals with access to complimentary credit monitoring for twenty-four (24) months and dedicated call center services as well as providing guidance on how to protect against identity theft and fraud, including advising individuals to report any suspected identity theft or fraud to their financial institutions. OutdoorSmart is also providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national credit reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for fraud and identity theft by reviewing account statements and monitoring credit reports, and encouragement to contact the Federal Trade Commission, their Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the Incident, please contact me at cyber@goodwinlaw.com.

Respectfully submitted,

Goodwin Procter LLP

/s/ *Kaitlin Betancourt*

Kaitlin Betancourt
Partner

KB

EXHIBIT A

(SEE ATTACHED)

OUTDOORsmart!

Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

<<VARIABLE DATA 1>>

Dear <<Full Name>>:

OutdoorSmart! Inc., which operates the Campfire Collective website, is writing to advise you of a recent event that may impact the security of certain personal information related to you. We write to provide you with information about the incident, the steps we have taken since discovering the incident, and the steps you can take to better protect your information should you feel it appropriate to do so.

What Happened? On November 3, 2025, Outdoor Smart was alerted to unusual activity on its Campfire Collective website and promptly initiated its incident response protocols. After an investigation, with the assistance of third-party cybersecurity specialists, Outdoor Smart identified the presence of unauthorized code capable of capturing payment card information used when making purchases on the Campfire Collective website. The unauthorized capturing of payment card information may have occurred between February 15, 2024 and November 4, 2025. Outdoor Smart immediately removed the unauthorized code on November 4, 2025.

Outdoor Smart has investigated this matter with the assistance of third party specialists and confirmed that the unauthorized code is no longer present. On December 4, 2025, Outdoor Smart confirmed that certain of your information might have been impacted in a recent security incident.

What Information Was Involved? The personal information involved may include your name, and payment card information, including card type <<Variable Data 2>>, card number, expiration date and CVC.

What We Are Doing. We take this event and the security of personal information in our care seriously. We moved quickly to respond and mitigate the issue and notify individuals. As part of our ongoing commitment to information security, we are reviewing our existing policies and procedures. As an added precaution, we are providing you with 24 months of complimentary access to credit monitoring and identity restoration services through Epiq as well as guidance on how to better protect your information. Enrollment information is contained in the attached *Steps You Can Take to Protect Personal Information***.** We are unable to enroll you in these services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Protect Personal Information*. There, you will find more information on the credit monitoring and identity restoration services we are making available to you. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have questions you may contact our dedicated assistance line at 888-367-0556, Monday through Friday from 9:00 am ET to 9:00 pm ET, excluding major U.S. holidays. You may also write to Outdoor Smart at Unit 2, 890 Taylor Creek Drive, Ottawa, Ontario K4A 0Z9.

Sincerely,

OutdoorSmart! Inc

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

<<Full Name>>
Activation Code: <<ACTIVATION CODE>>
Enrollment Deadline: <<ENROLLMENT DEADLINE>>
Coverage Length: 24 Months

Epiq - Privacy Solutions ID
3B Credit Monitoring

How To Enroll:

1) Visit www.privacysolutionsid.com and click "Activate Account"
2) Enter the following activation code, **<<Activation Code>>** and complete the enrollment form
3) Complete the identity verification process
4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
5) Enter your log-in credentials
6) You will be directed to your dashboard and activation is complete!

Product Features:

3-Bureau Credit Monitoring with Alerts
Monitors your credit file(s) with each of the 3 Credit Bureaus for key changes, with alerts such as credit inquiries, new accounts, and public records.

VantageScore® 3.0 Credit Score with Score Tracker[1]
1-Bureau VantageScore®3.0 (monthly) and Credit Score Tracker.

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)
Detect and prevent common identity theft events outside of what is on your credit report. Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, online document signings and payment platforms, with alerts.

Dark Web Monitoring
Scans millions of servers, online chat rooms, message boards, and websites across all sides of the web to detect fraudulent use of your personal information, with alerts.

Change of Address Monitoring
Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users' current or past addresses.

Credit Protection
3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Personal Info Protection
Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers – so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

Identity Restoration & Lost Wallet Assistance
Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

Up to $1M Identity Theft Insurance[2]
Provides up to $1,000,000 ($0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer- UEFT[2]
Provides up to $1,000,000 ($0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity (occurrence based).

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 3B Credit Monitoring, please call directly at **866.675.2006**, Monday-Friday 9:00 a.m. to 5:30 p.m., ET.

1 The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore® credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

2 Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. or American Bankers Insurance Company of Florida, an Assurant company. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

*For Iowa Residents***:** Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut St., Des Moines, IA 50319, Telephone: 515-281-5164, www.iowaattorneygeneral.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately <<Rhode Island Count>> Rhode Island residents that may be impacted by this event.