



January 16, 2025

BY EMAIL

**Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202**

To Whom It May Concern:

First Advantage Enterprise Screening Corporation (“First Advantage”) is providing this notice of a cybersecurity event to your office. First Advantage specializes in employment background screening and identity verification services.

On December 10, 2024, First Advantage discovered that certain personal information associated with a small number of First Advantage Profile Advantage accounts was being sold on a darkweb site. Profile Advantage is a candidate data entry portal primarily used to initiate background screening for employment purposes. First Advantage promptly launched an investigation and determined that, on or about November 12, 2024, an unauthorized third party gained access to a small number of Profile Advantage accounts using valid log-in credentials. Leveraging this access, the threat actor was then able to remove certain personal information associated with the affected Profile Advantage accounts.

On December 17, 2024, First Advantage determined that approximately 16 Maryland residents were affected. The affected information consisted of each individual’s first name, last name, Social Security number, driver’s license number, email address, and Profile Advantage password. There is no evidence that the account credentials used by the unauthorized third party were obtained from First Advantage’s network. First Advantage has not received any confirmed reports of this personal information being used for fraud or identity theft purposes.

First Advantage began sending formal notification to the affected individuals via U.S. mail on January 16, 2025. Attached is a copy of the consumer notification mailed to the affected individuals in your state. First Advantage is providing affected individuals with 24 months of complimentary credit monitoring and identity theft protection services through Experian. We have also established a dedicated call center to answer individuals’ questions.

We have also taken, and will continue to take, proactive measures to protect our systems and data. Specifically, upon discovering the incident, First Advantage promptly reset all compromised credentials and mandated multi-factor authentication for all Profile Advantage accounts beginning on December 23, 2024.

If you have any questions, please contact me at bret.jardine@fadv.com.

Regards,

Bret Jardine

Chief Legal Officer and Corporate Secretary

First Advantage Enterprise Screening Corporation



<<Date>>

<<First Name>> <<Middle Name>> <<Last Name>> <<Suffix>>
<<Address 1>>
<<Address 2>>
<<City>> <<State>> <<Zip Code>>

<<Variable Text 1 (Notice of /Data Breach / Security Incident)/>>

Dear <<First Name>>:

We are writing to let you know of a cybersecurity incident that affected certain of your personal information stored in your First Advantage Enterprise Screening Corporation ("First Advantage") Profile Advantage account. We are providing you with information about the incident, our response, and additional measures you can take to help protect yourself.

What Happened?

On or about November 12, 2024, an unauthorized third party gained access to a small number of Profile Advantage accounts using valid log-in credentials. On December 10, 2024, we became aware of the unauthorized activity and promptly activated our response process, launching an investigation into the nature of the issue.

There is no evidence that your log-in credentials were taken from First Advantage, and we recommend changing passwords for any other accounts that use the same email address as a username and the same password.

What Information Was Involved?

First Advantage has determined that your name, Social Security number, driver's license number, email address, and password to your Profile Advantage account were affected by this incident.

What We Are Doing.

As part of our response, we have reset account credentials for all affected consumers and implemented additional security measures to strengthen the ongoing security of Profile Advantage accounts.

We have not received any confirmed reports of this personal information being used for fraud or identity theft purposes as a result of this incident. As an additional precaution, we are offering you two years of complimentary credit monitoring and identity restoration services through Experian. Details about this offer and instructions on how to activate these services are enclosed with this letter. You must enroll by April 30, 2025 to use these services.

What You Can Do.

We encourage you to remain vigilant and review your account statements and free credit reports regularly to ensure there is no unauthorized or unexplained activity. We also encourage you to enroll in the complimentary credit monitoring services that we are offering. Please review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains details about this offer and general guidance on what you can do to safeguard against possible future misuse of your information.

For More Information.

First Advantage has established a dedicated call center to answer questions about this incident. If you have any questions regarding this incident, please call <<Call Center Number>>, Monday through Friday 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

First Advantage

Steps You Can Take to Help Protect Personal Information

Enroll in Experian's Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

We encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- **Enroll by 5:59pm CT on April 30, 2025** (Your code will not work after this date).
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: <<Variable 2 (Activation Code)>>

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to Experian. If, after discussing your situation with an Experian agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is immediately available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

If you have questions about the product, need assistance with Identity Restoration as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-931-7577 by April 30, 2025. Be prepared to provide engagement number B138597 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.

- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. 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 1-877-322-8228 toll-free. 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 one-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/credit
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5069	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the three major credit reporting bureaus, the Federal Trade Commission, or your 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Iowa residents, you are advised to report any suspected identity theft to law enforcement, including local law enforcement or the Iowa Attorney General. The Iowa Attorney General may be contacted at 1305 E. Walnut Street, Des Moines, IA 50319; 1-515-281-5926 or 1-888-777-4590; and www.iowaattorneygeneral.gov

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and [https://www.marylandattorneygeneral.gov/](http://www.marylandattorneygeneral.gov/).

For Massachusetts residents, under Massachusetts law, individuals have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

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; and <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.