EXHIBIT 2

We continue to represent American InfoSource ("AIS") located at 5847 San Felipe, Suite 1200 Houston, TX 77057, and are writing to supplement our June 30, 2025, notification to your office regarding an incident that may affect the security of certain personal information relating to an additional five (5) Maine residents. Our previous notification to your office is attached as ***Exhibit AA.*** This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, AIS does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

AIS provides various services for financial institutions that involves the hosting and processing of certain consumer information on behalf of those institutions. On February 17, 2025, AIS identified suspicious activity in its IT environment and shut down its environment in an abundance of caution. AIS immediately initiated an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity and restore systems in a secure manner. The investigation revealed that the earliest known unauthorized activity in AIS' systems occurred on February 16, 2025, and no further suspicious activity was detected after February 21, 2025. Through the investigation, AIS determined that an unauthorized actor had gained access to its environment and took certain information from two employee systems. Therefore, AIS retained a third-party firm to complete a comprehensive review of the incident that included a determination of the data involved and to whom the data belonged. On May 15, 2025, AIS determined that information related to certain individuals could be affected and worked to gather sufficient address information so that direct notice could be provided. On June 13, 2025, AIS had sufficient information to begin providing direct notice to impacted individuals. On July 9, 2025, AIS received sufficient confirmation of the information to allow us to provide direct notice to these additional impacted individuals.

The information that could have been subject to unauthorized access includes name, Social Security number, and financial account number.

Notice to Maine Residents

On June 30, 2025, AIS began providing written notice of this incident to Maine residents. On July 21, 2025, AIS continued providing notice of this incident to an additional five (5) Maine Residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit BB***.

Other Steps Taken and To Be Taken

Upon discovering the event, AIS moved quickly to investigate and respond to the incident, assess the security of AIS systems, and identify potentially affected individuals. Further, AIS notified federal law enforcement regarding the event. AIS is also working to implement additional safeguards and training to its employees. AIS is providing access to credit monitoring services for twelve (12) months, through Equifax to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, AIS is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. AIS is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

AIS is providing written notice of this incident state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT AA

Form Submitted

✓ **Form submitted successfully.**

Thank you for submitting the breach details through this reporting form. The information you have provided has been submitted to the agency.

Please close this browser window.

Produced Files

Attached File(s)

Download All

Download Submission

Continue

Maine Security Breach Reporting Form

6/30/2025 5:19:05 PM

Maine Security Breach Reporting Form

Pursuant to the Notice of Risk to Personal Data Act (Maine Revised Statutes 10 M.R.S.A. §§1346-1350-B)

Entity that owns or maintains the computerized data that was subject to the breach:

Type of Organization: Other Commercial

Entity Name: AIS InfoSource

Entity Address

Address Line 1: 5847 San Felipe

Address Line 2: Suite 1200

City: Houston

State: Texas

Zip: 77057

Submitted by:

Name: Tom Moran

Title: Partner

Firm name: Mullen Coughlin LLC

Telephone Number: (267) 930-2085

Email Address: tmoran@mullen.law

Relationship to Entity: Counsel

Breach Information:

Total Number of Persons Affected: -

Total number of Maine Residents Affected : 8

If the number of Maine residents exceeds 1,000, have the consumer reporting agencies been notified?:

- [ ] Yes
- [ ] No

Date(s) Breach Occurred: 02/16/2025

Date Breach Discovered: 06-13-2025

Description of the Breach (please check all that apply):

- [ ] Loss or theft of device or media (computer, laptop, external hard drive, thumb drive, CD, tape, etc.)
- [ ] Internal system breach
- [ ] Insider wrongdoing
- [X] External system breach (hacking)
- [ ] Inadvertent disclosure
- [ ] Other

Information Acquired - Name or other personal identifier in combination with (please check all that apply):

- [X] Social security number
- [ ] Driver's license number or state identification card number
- [X] Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords
- [ ] Account passwords or personal identification numbers or other access codes
- [ ] Any of the data elements contained in paragraphs A to D when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

Notification and Protection Services:

Type of notification: Written

Date(s) of consumer notification: 06/30/2025

Please attach a copy of the template of the notice to affected Maine residents. Please ensure all uploaded documents meet Web Content Accessibility Guidelines (WCAG) and can be viewed (website updated nightly).

Upload Template of Notice: AIS InfoSource - Notice of Data Event - ME.pdf

List dates of any previous (within 12 months) breach notifications:

Were identity theft protection services offered?:

- [X] Yes
- [ ] No

Identity Theft Service Description: 12 months of credit monitoring and identity protection through Equifax.

Review

Review

Type of Organization: Other Commercial

Entity Name: AIS InfoSource

Entity Address

Address Line 1: 5847 San Felipe

Address Line 2: Suite 1200

City: Houston

State: Texas

Zip: 77057

Name: Tom Moran

Title: Partner

Firm name: Mullen Coughlin LLC

Telephone Number: (267) 930-2085

Email Address: tmoran@mullen.law

Relationship to Entity: Counsel

Total Number of Persons Affected: -

Total number of Maine Residents Affected : 8

Date(s) Breach Occurred: 02/16/2025

Date Breach Discovered: 06-13-2025

Description of the Breach (please check all that apply):

- [ ] Loss or theft of device or media (computer, laptop, external hard drive, thumb drive, CD, tape, etc.)
- [ ] Internal system breach
- [ ] Insider wrongdoing
- [X] External system breach (hacking)
- [ ] Inadvertent disclosure
- [ ] Other

Information Acquired - Name or other personal identifier in combination with (please check all that apply):

[X] Social security number

[ ] Driver's license number or state identification card number

[X] Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords

[ ] Account passwords or personal identification numbers or other access codes

[ ] Any of the data elements contained in paragraphs A to D when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

Type of notification: Written

Date(s) of consumer notification: 06/30/2025

Upload Template of Notice: AIS InfoSource - Notice of Data Event - ME.pdf

Were identity theft protection services offered?:

[X] Yes

[ ] No

Identity Theft Service Description: 12 months of credit monitoring and identity protection through Equifax.

Disclosure and Agreement

By checking the box below, you certify that all information supplied on this form is true and accurate to the best of your knowledge.

[X] The disclosure statement has been read and agreed to by the individual submitting this Maine Attorney General Reporting Form.

Maine Security Breach Reporting Form

✔ Maine Security Breach Reporting Form

⚠ Review

Pursuant to the Notice of Risk to Personal Data Act (Maine Revised Statutes 10 M.R.S.A. §§1346-1350-B)

Entity that owns or maintains the computerized data that was subject to the breach:

Type of Organization (Please select one) *

Other Commercial

Entity Name *

AIS InfoSource

Entity Address *

5847 San Felipe

Suite 1200

Houston

Texas

77057

Submitted by:

Name *

Tom Moran

Title *

Partner

Firm name (if different than entity name)

Mullen Coughlin LLC

Telephone Number *

(267) 930-2085

Email Address *

tmoran@mullen.law

Relationship to entity whose information was compromised *

Counsel

Breach Information:

Total number of persons affected (including Maine residents) *

-

Total number of Maine residents affected *

8

If the number of Maine residents exceeds 1,000, have the consumer reporting agencies been notified?

- ○ Yes
- ○ No

Date(s) Breach Occurred *

02/16/2025

Date Breach Discovered *

06-13-2025

Description of the Breach (please check all that apply)*

- ☐ Loss or theft of device or media (computer, laptop, external hard drive, thumb drive, CD, tape, etc.)
- ☐ Internal system breach
- ☐ Insider wrongdoing
- ☑ External system breach (hacking)
- ☐ Inadvertent disclosure
- ☐ Other

Information Acquired - Name or other personal identifier in combination with (please check all that apply)*

- ☑ Social security number
- ☐ Driver's license number or state identification card number
- ☑ Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords
- ☐ Account passwords or personal identification numbers or other access codes
- ☐ Any of the data elements contained in paragraphs A to D when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

Notification and Protection Services:

Type of notification *

Written

Date(s) of consumer notification *

06/30/2025

Please attach a copy of the template of the notice to affected Maine residents. Please ensure all uploaded documents meet Web Content Accessibility Guidelines (WCAG) and can be viewed (website updated nightly).

Upload Template of Notice

List dates of any previous (within 12 months) breach notifications

mm/dd/yyyy

Were identity theft protection services offered?*

- ◉ Yes
- ○ No

If yes, please provide the duration, the provider of the service and a brief description of the service *

12 months of credit monitoring and identity protection through Equifax.

EXHIBIT 1

By providing this notice, AIS InfoSource LP ("AIS") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On February 17, 2025, AIS identified suspicious activity in its' IT environment and shut down its' environment in an abundance of caution. AIS immediately initiated an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity and restore systems in a secure manner. The investigation revealed that the earliest known unauthorized activity in AIS' systems occurred on February 16, 2025, and no further suspicious activity was detected after February 21, 2025. Through the investigation, AIS determined that an unauthorized actor had gained access to its' environment and took certain information from two employee systems. Therefore, AIS retained a third-party e-discovery firm to complete a comprehensive review of the data which may be at risk to determine what information was at issue and to whom the information related. On May 15, 2025, AIS determined that information related to certain individuals could be affected and worked to gather sufficient address information so that direct notice could be provided. On June 13, 2025, AIS had sufficient information to begin providing direct notice to impacted individuals.

The information that could have been subject to unauthorized access includes name, Social Security number, and financial account number.

Notice to Maine Residents

On June 30, 2025, AIS began providing written notice of this incident to eight (8) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, AIS moved quickly to investigate and respond to the incident, assess the security of AIS systems, and identify potentially affected individuals. Further, AIS notified federal law enforcement regarding the event. AIS is also working to implement additional safeguards and training to its employees. AIS is providing access to credit monitoring services for twelve (12) months, through Equifax, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, AIS is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. AIS is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

AIS is providing written notice of this incident to state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

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

<Date>

NOTICE OF <<SECURITY INCIDENT/ DATA BREACH>>

Dear <<Full Name>>:

AIS InfoSource LP ("AIS") writes to inform you of an incident that involves some of your information. This letter provides an overview of the incident, our response, and steps you may take to better protect yourself should you wish to do so.

What Happened? On February 17, 2025, AIS identified suspicious activity in our network and promptly took measures to mitigate the risk of further activity. AIS quickly initiated an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity. The investigation revealed that the earliest known unauthorized activity in our systems occurred between February 16, 2025, and February 21, 2025. Through the investigation, we determined that an unauthorized actor gained access to our environment and took a limited subset of data. Therefore, AIS retained a third-party to complete a comprehensive review of the data involved to determine what information was at issue and to whom it belonged. On May 15, 2025, AIS determined that information related to you was included in the data and worked to gather contact information so that direct notice could be provided. On June 13, 2025, AIS received sufficient information to provide direct notice to you.

What Information Was Involved? The information that could have been impacted includes your name and the following types of information: <<Data Elements>>.

What We Are Doing. AIS takes the confidentiality, privacy, and security of information in its care very seriously. Upon discovering the incident, we took immediate steps to secure the network and strengthen our security posture moving forward. AIS is also offering you access to complimentary credit monitoring and identity restoration services through Equifax for <<12 / 24 months>>. The deadline to enroll in these services is <<Enrollment Deadline>>. Please note that you will need to enroll yourself in these services, as we are not able to do so on your behalf. You can find instructions regarding how to enroll in these services in the enclosed *Steps You Can Take to Protect Personal Information*.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Personal Information* which contains guidance regarding what you can do to better protect against possible misuse of your information. We also 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. We encourage you to report any suspected incidents of identity theft or fraud to your credit card company or bank.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, please call 855-361-0323. Monday through Friday from 8:00 am to 8:00 pm Central Time. You may also write to AIS at 5847 San Felipe, Suite 1200 Houston, TX 77057.

Sincerely,
AIS

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

EQUIFAX®

Enter your Activation Code: <*ACTIVATION CODE*>
Enrollment Deadline: <Enrollment *Deadline* >

Equifax Credit Watch™ Gold
*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of ***<ACTIVATION CODE>*** then click "Submit" and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click "Continue".
If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout**:

Upon successful verification of your identity, you will see the Checkout Page.
Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. [2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com [4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. 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 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 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/. You may also write to AIS at 5847 San Felipe, Suite 1200 Houston, TX 77057.

For Massachusetts residents, Under Massachusetts law, you 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; 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. You may also write to AIS at 5847 San Felipe, Suite 1200 Houston, TX 77057.

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 residents that may be impacted by this event.

EXHIBIT BB

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

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

<Date>

NOTICE OF <<SECURITY INCIDENT/ DATA BREACH>>

Dear <<Full Name>>:

AIS InfoSource LP ("AIS") writes to inform you of an incident that involves some of your information. This letter provides an overview of the incident, our response, and steps you may take to better protect yourself should you wish to do so.

Who is AIS and Why Did They Have My Information? AIS provides various services for financial institutions related to bankruptcy notifications and proceedings, deceased notifications and probate services. AIS was in possession of your information in connection with one or more of these services for one of its financial institution clients.

What Happened? On February 17, 2025, AIS identified suspicious activity in our network and promptly took measures to mitigate the risk of further activity. AIS quickly initiated an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity. The investigation revealed that the earliest known unauthorized activity in our systems occurred between February 16, 2025, and February 21, 2025. Through the investigation, we determined that an unauthorized actor gained access to our environment and took a limited subset of data. Therefore, AIS retained a third-party to complete a comprehensive review of the data involved to determine what information was at issue and to whom it belonged. On May 15, 2025, AIS determined that information related to you was included in the data and worked to gather contact information so that direct notice could be provided. On July 9, 2025, AIS received sufficient information to provide direct notice to you.

What Information Was Involved? The information that could have been impacted includes your name and the following types of information: <<Data Elements>>.

What We Are Doing. AIS takes the confidentiality, privacy, and security of information in its care very seriously. Upon discovering the incident, we took immediate steps to secure the network and strengthen our security posture moving forward. AIS is also offering you access to complimentary credit monitoring and identity restoration services through Equifax for <<12 / 24 months>>. The deadline to enroll in these services is <<Enrollment Deadline>>. Please note that you will need to enroll yourself in these services, as we are not able to do so on your behalf. You can find instructions regarding how to enroll in these services in the enclosed *Steps You Can Take to Protect Personal Information*.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Personal Information* which contains guidance regarding what you can do to better protect against possible misuse of your information. We also 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. We encourage you to report any suspected incidents of identity theft or fraud to your credit card company or bank.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, please call 855-361-0323, Monday through Friday from 8:00 am to 8:00 pm Central Time. You may also write to AIS at 5847 San Felipe, Suite 1200 Houston, TX 77057.

Sincerely,
AIS

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

EQUIFAX®

Enter your Activation Code: <*ACTIVATION CODE*>
Enrollment Deadline: <Enrollment *Deadline* >

Equifax Credit Watch™ Gold
*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of ***<ACTIVATION CODE>*** then click "Submit" and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click "Continue".
If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout**:

Upon successful verification of your identity, you will see the Checkout Page.
Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. [2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com [4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. 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 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 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/. You may also write to AIS at 5847 San Felipe, Suite 1200 Houston, TX 77057.

For Massachusetts residents, under Massachusetts law, you 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; 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. You may also write to AIS at 5847 San Felipe, Suite 1200 Houston, TX 77057.

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 residents that may be impacted by this event.