EXHIBIT 1

This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Valsoft Corporation Inc. d/b/a AllTrust ("Alltrust") does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

Nature of the Data Event

On February 14, 2024, Alltrust became aware of unusual activity on a non-production computer network which is owned and managed by their subsidiary Aspire USA, LLC ("Aspire"). Aspire's internal security team identified an in-progress file transfer which they were able to interrupt mid-transfer.

Aspire immediately took steps to secure the impacted network and launched an investigation with third-party cybersecurity and forensic specialists to determine the nature and scope of the activity. The investigation determined that an unauthorized actor accessed their network between February 12, 2024, and February 15, 2024, and took certain files within their network during that time. While the investigation was able to confirm that certain systems were accessed, it was unable to confirm which specific files within those systems were actually accessed or taken. Aspire also believes their immediate actions stopped the activity in process and that there is minimal risk of harm to individuals. Out of an abundance of caution, Aspire, with the assistance of third-party specialists, conducted a comprehensive and through programmatic and manual review of the contents of the impacted system to determine whether sensitive information may have been present at the time of the event.

The review determined that information related to certain individuals was present on the impacted system. Following this review, Alltrust undertook additional in-depth review of its internal files to identify the individuals and AllTrust customers to which the information belongs and to confirm the identities and contact information for potentially affected individuals in order to provide notification. This process was recently completed.

Aspire then undertook the vetting and retention of a third-party notification services provider to assist with the printing and mailing of notification letters, staffing of a toll-free call center to address questions from notified individuals, and the provision of complimentary credit monitoring services. The individual notification population and address information compiled by Aspire was subsequently provided to the notification services provider, discussed above, and correlated with the National Change of Address ("NCOA") database. On February 26, 2025, the NCOA search results were provided to Aspire for further analysis and confirmed that Nebraska residents had been impacted by the event.

The information that could have been subject to unauthorized access includes name, Social Security number, driver's license number, state-issued identification number, and financial account information.

Notice to Nebraska Residents

On or about February 27, 2025, Alltrust provided written notice of this incident to ninety-nine (99) Nebraska 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 becoming aware of the event, Alltrust immediately took steps to confirm the security of their systems and to determine what information was potentially impacted. Alltrust implemented additional security measures, including those required to obtain SOC2 compliance, and is reviewing existing security policies to further protect against similar incidents moving forward. Alltrust is providing access to credit monitoring services for twelve (12) months, through IDX, a ZeroFox company, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Alltrust 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. Alltrust 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.

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

EXHIBIT A

P.O. Box 1907
Suwanee, GA 30024

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/AllTrust

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

VIA U.S. MAIL

February 27, 2025

Notice of Data <<Variable Data 1>>

Dear <<Name 1>> <<Name 2>>:

Valsoft Corporation Inc. d/b/a AllTrust ("**AllTrust**") is writing to notify you of a data security incident that may involve some of your personal information. Upon becoming aware of this event, we immediately implemented our incident response plan, engaged specialists to assist in our investigation, implemented additional safeguards within our environment, and coordinated with law enforcement. While we remain unaware of any actual misuse of information, we are writing to make you aware of the incident, the steps we are taking in response, and steps you may take to help protect your personal information, should you feel it is appropriate to do so.

What Happened? On February 14, 2024, we became aware of unusual activity on a non-production computer network which is owned and managed by our subsidiary Aspire USA, LLC ("**Aspire**"). Our internal security team identified an in-progress file transfer which they were able to interrupt mid-transfer.

Aspire immediately took steps to secure the impacted network and launched an investigation with third-party cybersecurity and forensic specialists to determine the nature and scope of the activity. The investigation determined that an unauthorized actor accessed our network between February 12, 2024, and February 15, 2024, and took certain files within our network during that time. While the investigation was able to confirm that certain systems were accessed, it was unable to confirm which specific files within those systems were actually accessed or taken. We also believe that our immediate actions stopped the activity in process. Out of an abundance of caution, Aspire, with the assistance of third-party specialists, conducted a comprehensive and time-intensive review of the contents of the impacted system to determine whether sensitive information may have been present at the time of the event.

Our review determined that information related to certain individuals was present on the impacted system. Following this review, we undertook additional in-depth review of our internal files to identify the individuals and AllTrust customers to which the information belongs. This process was recently completed.

What Information Was Involved? Our review determined that the following types of information were present on the impacted system at the time of the event: your name, <<Variable Data 3>>. Please note that we are not aware of any information which has been subject to actual misuse as a result of this event, and we are notifying you out of an abundance of caution.

What We Are Doing. The confidentiality, privacy, and security of information in our care is one of our highest priorities. Upon becoming aware of this incident, we immediately took steps to confirm the security of our systems and to determine what information was potentially impacted. We implemented additional security measures, and we are reviewing existing security policies to further protect against similar incidents moving forward. We are notifying potentially impacted individuals and organizations and reported this incident to federal law enforcement.

As an added precaution, we are offering you complimentary access to <<Membership Offering Length>> months of credit monitoring services, through IDX. You will need to enroll yourself in these services if you wish to do so, as we are not able to activate them on your behalf. Please review the instructions contained in the attached *Steps You Can Take to Protect Personal Information* for additional details on these services.

What You Can Do. AllTrust encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and monitor free credit reports for suspicious activity and to detect errors. We also encourage you to review the enclosed *Steps You Can Take to Protect Personal Information* and enroll in the credit monitoring services we are offering. While AllTrust will cover the cost of these services, you will need to follow the enrollment instructions to enroll in the services. Enrollment instructions are enclosed with this letter.

For More Information. If you have questions about this matter, you may contact our dedicated assistance line at 1-866-902-1994, Monday through Friday from 8:00 am to 8:00 pm Central Time, (excluding major U.S. holidays).

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Omar Zelaya-Velasquez
General Manager

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

Website and Enrollment. Scan the QR image or go to https://response.idx.us/AllTrust and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the enrollment deadline is May 27, 2025.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-866-902-1994 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

We advise you to remain vigilant against identity theft and fraud by reviewing all account statements and monitoring free credit reports. If you discover or suspect fraudulent activity involving your account, credit or debit card, we encourage you to promptly contact the issuing bank or relevant financial institution. The number to call for assistance is usually on the back of the card.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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-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 Fraud Alert, 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 Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your 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, DC 20001; 1-202-727-3400; and oag@dc.gov. AllTrust is located at 45150 Russell Branch Parkway Suite 201D Ashburn, VA 20147.

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/. AllTrust is located at 45150 Russell Branch Parkway Suite 201D Ashburn, VA 20147.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your 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 your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You 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 you to review your 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 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, you have the right to obtain any police report filed in regard to this incident. There are approximately <<#>> Rhode Island residents that may be impacted by this event.