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 Maine law, the applicability of the Maine 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 amd 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 Maine 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, and financial account information.

## Notice to Maine Residents

On or about February 27, 2025, Alltrust provided written notice of this incident to one hundred eighty-eight (188) 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 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.