EXHIBIT 1

By providing this notice, Crimson 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 June 30, 2024, Crimson became aware of a cyber security incident in which an unauthorized third party gained access to certain systems in Crimson's network. Upon becoming aware of this incident, Crimson initiated an investigation into the nature and scope of the incident. The investigation determined that certain information on Crimson's systems may have been viewed or taken without authorization between June 26, 2024 – June 30, 2024.

On or around July 15, 2024. Crimson determined that some of the information involved may have included personal information. On August 19, 2024, Crimson began providing written notice to the initial set of individuals identified.

Following additional data review, on or around November 8, 2024, Crimson identified additional individuals whose personal information was present in the data involved.

The information that could have been subject to unauthorized access may include name, financial account information and payment card information.

Notice to Maine Residents

On or about December 13, 2024, Crimson provided written notice of this incident to twenty-one (21) 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, Crimson moved quickly to investigate and respond to the incident, assess the security of Crimson systems, and identify potentially affected individuals. Further, Crimson notified federal law enforcement regarding the event. Crimson is also working to implement additional safeguards and training to its employees. Crimson is providing access to credit monitoring services for one (1) year, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Crimson 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. Crimson 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.