

<<Return Address>>
<<City>>, <<State>> <<Zip>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Notice of Data Security Incident at Stretto

Dear <<First Name>> <<Last Name>>,

As you may be aware, Stretto Inc. (“Stretto”) serves as the Claims and Noticing Agent for *In re: Celsius Network, LLC*, Case No. 22-10964 (MG), which is currently pending in the United States Bankruptcy Court for the Southern District of New York:

What Happened:

Stretto recently experienced a security incident regarding data held in connection with this case. A notice has been filed on the court docket with the Case No. 22-10964 (MG):

<https://cases.stretto.com/public/x191/11749/PLEADINGS/1174904262480000000141.pdf>

We are notifying you as we have confirmed that your data was accessed by an unauthorized party. In addition to your name, your mailing address, or phone number may have been included in this data. In some cases, the data related to Claim submissions may have contained amounts and other information provided by the creditor. However, our investigation did not find evidence that your SSN / TIN was impacted.

Please remain vigilant of potential security risks, such as phishing attempts. If you receive an email that appears to be from Celsius or Stretto, please verify the sender before you reply or click any links. If you have any questions relating to this security incident, please email CelsiusInquiries@stretto.com.

Sincerely,
Stretto

Stretto Logo

<<Return Address>>
<<City>>, <<State>> <<Zip>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Dear <<First Name>> <<Last Name>>,

As you may be aware, Stretto Inc. ("Stretto") serves as the Claims and Noticing Agent for *In re: Voyager Digital Holdings, Inc. et al.*, Case No. 22-10943 (MEW), currently pending in the United States Bankruptcy Court for the Southern District of New York. We are writing to advise you of a data security incident at Stretto that involved some of your personal information.

On April 17, 2024, Stretto information technology staff were alerted to suspicious activity occurring in one employee account. Stretto immediately initiated an internal investigation, which preliminarily determined that the account had been subject to unauthorized access. In response to this discovery, Stretto disabled all access by this account to Stretto systems and changed the password to the account.

Stretto engaged external cybersecurity professionals to conduct a thorough and detailed investigation of the Incident. A critical focus of the investigation was to identify the extent to which information held by Stretto in connection with the Voyager Bankruptcy Matter may have been impacted. Stretto's cybersecurity professionals completed their investigation on May 6, 2024. Immediately thereafter, Stretto conducted an exhaustive review of the documents which may have been affected by the incident. This review determined that information related to creditors in the Voyager Bankruptcy Matter may have been impacted.

We are notifying you as we have confirmed that your data was accessed by an unauthorized party. This data may have included your name, mailing address, e-mail address, fax number, phone number, claim amount, and/or schedule amount. In some cases, the data related to Claim submissions may have contained amounts and other information provided by the creditor. However, our investigation **did not** find evidence that your SSN / TIN was impacted.

We have no evidence indicating that your information has been misused. Nevertheless, we encourage you to remain vigilant of potential security risks, such as phishing attempts. If you receive an email that appears to be from Voyager or Stretto, please verify the sender before you reply or click any links.

Stretto