From: **LC Bulletin** <lc-bulletin@lclark.edu>

Date: April 11, 2023

Addressing Concerns About Compromised Data

Dear students, staff, and faculty,

A number of questions and concerns regarding the data posted by the cybercriminals who attacked the LC network have surfaced in the last few weeks. New information has been added to the FAQs to help provide additional support to the community: https://www.lclark.edu/news/march-2023/.

It is now clear that some amount of personal information belonging to the members of the LC community is included in the data. The full nature and scope of that data is not yet known and will not be confirmed until the investigation by our external experts is completed.

Our forensic experts are undertaking a process that is methodical and painstaking. It wasn't until this week that they were able to safely and successfully download the illegally stolen data from the “dark web.” They are currently scanning it for malicious content to ensure it is safe to analyze. The data will then be thoroughly and carefully reviewed, and any person whose protected personal information is found to have been included in the data will receive a formal legal notice. The same services that are being offered to current students and employees will be offered to anyone whose protected private information was compromised in this attack.

While necessary to protect the community, we regret the lengthiness of this process and know it is a source of frustration. It is unsettling to wonder and not know if your personal information has been compromised. That is why we have taken the proactive step of offering complimentary credit monitoring to all current students and employees now, choosing not to wait for the full retrieval and confirmation of data to provide this assistance.

Credit monitoring is the most important step you can take to protect yourself. In addition to monitoring, the services provided include identity restoration support and identity theft insurance for anyone experiencing an incidence of fraud. We urge you to sign up for these services by filling out this short request form. After you submit the form, you will automatically receive an email from the address "IT Enterprise Applications team," with the subject "Credit Monitoring Request Submitted,” which will include an enrollment code, additional details on services provided, and instructions on how you can activate the services. **This automatic email response is not spam.**

We are aware that a number of individuals report discovering that their social security numbers have been used to fraudulently file a tax return. We have added information to the FAQ page with a link to information from the IRS about how to handle such a situation.

We are also aware that concerned members of the community have searched the “dark web” and identified data that may now be circulating. Accessing stolen, illegal information from the “dark web” carries risks for those who access and distribute it. It could also facilitate additional criminal and malicious activity targeting our community. It is for these reasons that we are asking you to refrain from accessing or distributing such material.

As always, thank you for your understanding and patience.

Sincerely,
The Executive Council