vcuarts QATAR

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<last_name>>:

Like many organizations around the world, the VCUarts Qatar ("VCUQ"), community has unfortunately become the victim of a cybersecurity incident. This message details what we know about the incident at this time and how it may potentially have affected your personal information.

VCUQ takes the privacy and security of your personal information very seriously and we sincerely regret any concern this incident may cause you. We have notified law enforcement in both Qatar and in the United States and intend to support any law enforcement investigation into this matter.

We take our obligation to safeguard personal information very seriously and are continuing to evaluate additional actions to strengthen our network security in the face of an ever-evolving cyber threat landscape.

What Happened

As we shared in a message to the VCUQ community on 4 July 2024, VCUQ was victimized by a sophisticated ransomware incident. We received information suggesting that some personal information may have been accessed or viewed during the ransomware incident on or about 2 July 2024. For the past few weeks, our technical team has coordinated with leading outside cybersecurity experts to further investigate and understand the scope of data implicated.

Based on this investigation, we have determined that some information pertaining to VCUQ vendors and visitors may have been accessed. In particular, the following types of information about you may have been accessed or viewed as a result of this incident: your name, date of birth, email address, address, telephone number, nationality, descriptive information about transactions between you and VCUQ (e.g., the nature of products or services that you have provided VCUQ and the amount that you were paid for them), and/or details concerning visits you may have made to the VCUQ campus, including itineraries and hospitality arrangements.

Importantly, information sufficient for accessing your personal financial accounts was **not** subjected to unauthorized access. We do not believe this information can be used in identity theft activities. However, we are notifying you of this incident out of an abundance of caution, and to flag the possibility that you might encounter a temporary increase in phishing email attempts.

What Actions We Have Taken

Upon discovering the incident, VCUQ initiated an investigation and engaged leading outside cybersecurity experts to determine the scope of the incident. External experts have confirmed that our information technology environment is presently secure.

What You Can Do

Given the nature of your information accessed in this incident, we do not believe that this incident places you at a heightened risk for identity theft or fraud. However, as with any data incident, there is the possibility that identity theft can occur. Please remain vigilant by regularly reviewing and monitoring account statements and credit reports to detect potential errors or fraud and identity theft that can possibly occur with a security incident.

If you experience potential incidents of identity theft, please report them to your local authorities.

For More Information.

If you have any further questions regarding this matter, please reach out to Chief Technology Officer Mirza Ahmed Baig at vcuqprivacy@vcu.edu or available via telephone at +974 4402 0571.

Please note that VCUQ is utilizing Kroll as a vendor to facilitate this notification. The return address on this letter is to Kroll return mailing processing.

We deeply regret that this incident occurred and are committed to supporting you.

Sincerely,

Amir Berbić
Dean
VCUarts Qatar