Notification of Technology Management Resources Security Incident

What happened? Surgical Specialty Center of Baton Rouge ("SSCBR") has a lockbox service with IBERIABANK for collecting and processing from our patients and/or customers. IBERIABANK uses Technology Management Resources, Inc. (TMR) as a third-party lockbox service provider to process payments and capture pertinent payment data for items received in the lockbox. On October 14, 2021, TMR identified unusual activity with a user account in its lockbox application. It was determined that the activity was unauthorized, and the account was promptly disabled. SSCBR was recently notified of this incident and has been actively seeking information regarding the incident to be able to provide this notice.

TMR investigated the incident and reported that the unauthorized activity occurred between October 12, 2021, and October 13, 2021. According to TMR's investigation, the threat actor accessed bytes that were associated with certain images for lockbox payments and related documents. TMR has stated that the bytes (bits of computer data) accessed by the threat actor were in binary format only and as an encoded string (this means that the data was an encoded series of information stored in the form of ones and zeros). Technical manipulation of the bytes would be required to convert them into images. No actual images were viewed by the threat actors during the period of unauthorized access. TMR determined that it is likely that these bytes were obtained by the threat actor based upon traffic to the IP address. TMR's investigation has not revealed any evidence to confirm that the threat actor converted the bytes into images, although this could have been possible.

What information was involved? According to TMR, the encoded data was associated with certain check images and related documents within TMR's client payment application (iRemit) that may have contained PII or PHI. Specifically, after completing e-discovery on these documents, the information potentially included may have included your name, address, account numbers, bank routing numbers, date of birth, social security number, drivers license, date of service, geographic identifiers, health insurance information, medical information, diagnosis/conditions, lab results, medications, patient account numbers, procedure type, provider name, student ID, treatment cost information and/or claims information.

What are SSCBR, IBERIABANK and TMR doing in response? We take the privacy and security of personal information very seriously. As part of our ongoing commitment to information privacy and the security of information, we are notifying you of this incident. Although we are not aware of any misuse of your information as a result of this incident, out of an abundance of caution, IBERIABANK is offering complimentary credit monitoring and identity theft protection through TransUnion. These services will be available for 12 months at no cost in order to give you peace of mind. You must complete the enrollment steps listed in your letter to activate these services.

What you can do. As a best practice, we encourage you to remain vigilant against incidents of identity theft and fraud, to review financial account statements, and to monitor credit reports for suspicious activity. You may also enroll in the complimentary credit monitoring and identity theft protection services IBERIABANK is making available to you as a professional courtesy and in an abundance of caution.

For more information. To verify and obtain additional information regarding whether your information was potentially affected by this incident, please call, 1-855-604-1755, toll-free, Monday through Friday, 9:00 am – 9:00 pm Eastern Time. We apologize for any inconvenience this 2021 lockbox service provider security incident may have caused you.