Technology Management Resources, Inc., Breach

Frequently Asked Questions

What happened?

On July 2, 2020, Technology Management Resources, Inc., (TMR) discovered that an employee's account credentials had been compromised by a cybercriminal who used the information to gain access to TMR's application and to view images containing Personal Health Information.

What is TMR?

TMR is a third-party lockbox provider used by IBERIABANK.

As a patient of Monroe Surgical Hospital, how does this affect me?

Monroe Surgical Hospital uses IBERIABANK's lockbox service to collect and processes payments from our patients and customers. In turn, IBERIABANK uses TMR to scan and process the payments and other pertinent payment data received in the lockbox. Monroe Surgical Hospital has no relationship with TMR.

What is a lockbox?

A lockbox is a service provided by banks to businesses for collecting and processing their customers' payments. IBERIABANK contracted with TMR to process payments and capture pertinent payment data for items received in the bank's lockbox.

What caused the security incident?

Based on the information provided by TMR, a cybercriminal, or threat actor, obtained the credentials of a TMR employee's account. The threat actor used the credentials to gain access into TMR's application and to view images of checks and other items containing potential PHI. The PHI on these images may have included certain patients' names, addresses, dates of birth, patient and health insurance account numbers, procedure type, provider name and treatment cost information.

When did the incident occur?

According to TMR, the threat actor viewed images between August 5, 2018 and May 31, 2020, with the bulk of the activity occurring between February and May 2020.

What information was involved?

The images viewed may have contained PHI, including certain patients' names, addresses, dates of birth, patient and health insurance account numbers, procedure type, provider name and treatment cost information.

Do you have any indication that my personal data has been compromised?

After completing an extensive discovery, TMR provided us with a list of all our patients whose PHI was potentially viewed by the threat actor during the incident.

Did the threat actor download the data?

TMR reports that it has found no evidence that any data was downloaded by the cybercriminal.

Is the identity of the threat actor known?

According to TMR, the threat actor gained unauthorized accesses to the TMR application from a German IP address. However, TMR has not learned the identity of the person responsible for the incident.

What is IBERIABANK doing in response to the incident?

IBERIABANK is offering credit monitoring and identity theft protection through CyberScout. Please see the letter sent to you by IBERIABANK for instructions on how to enroll.

What has TMR done in response to the incident?

TMR reported that when they discovered the incident, they immediately secured the account and began an investigation in consultation with external cybersecurity professionals. TMR also notified the FBI of this incident. They believe the incident is part of a wider effort by an unknown cybercriminal to attack TMR customers beyond IBERIABANK.

TMR reports that it has taken several corrective actions to remediate the security incident, prevent a further security incident and mitigate the effects of this security incident. According to TMR, its credentials have been reset or deactivated (as applicable). TMR also reports that it implemented additional rules in its firewall to more tightly control the ability to access its application from other countries, among other steps taken.

What should I be doing?

As a best practice, we encourage our patients and customers to remain vigilant against incidents of identity theft and fraud. Review your financial account statements and claims information from your health insurance provider and monitor credit reports for suspicious activity. If you find any suspected

issues related to this incident you should notify the proper law enforcement authorities and report them to IBERIABANK by calling toll-free 1-888-905-0513 Monday through Friday, 8 a.m. to 8 p.m.

You can also use this toll-free number if you do not receive a letter from IBERIABANK but are still concerned that your information was potentially affected by this incident.