

Medical provider waited months to send patients letters about ransomware attack

<https://www.khou.com/article/news/investigations/medical-provider-ransomware-attack-gastroenterology-consultants/285-433d27bc-5351-4962-9cc0-97e54d3a3201>

BY: Jeremy Rogalski

September 9, 2021

When the letter finally arrived, it contained unsettling news about a deal struck with the hackers.

HOUSTON — A local health care provider attacked by a ransomware virus did not send letters to patients informing them of the data breach for months, KHOU 11 Investigates has confirmed.

Gastroenterology Consultants mailed notices to more than 161,000 patients on Aug. 6, informing them of a “data security incident” that occurred on Jan. 10.

“It’s just ridiculous,” patient Amber Wietlispach said.

But the delayed notification is not the thing upsetting patients. The letter also indicated the company paid the hackers ransom money and then trusted the criminals to keep their word about deleting the data.

“Based on our negotiated resolution with the attacker, we received assurances that any potential exfiltrated data had been destroyed,” the letter stated.

For Wietlispach, the so-called assurances do not offer any peace of mind.

“You can pay them off, but how do you know? How do you know that they really got rid of your information?” she said. “How do you trust somebody that you had to pay money to?”

Gastroenterology said only a fraction of its patients had their social security numbers compromised, and the hacked data was limited to names, addresses and some personal health information. The company said its patient medical record system was not impacted by the incident.

“Gastroenterology immediately changed all passwords, disconnected its systems and launched a full forensic investigation to determine the nature and scope of the incident to understand the vulnerability of its network,” the company said in a statement.

However, the company did not promptly report the hack to state authorities. Under Texas law, businesses are required to notify the Attorney General’s Office within 60 days of any data breach affecting more than 250 people. Records provided by Gastroenterology show that notification didn’t occur until August 9, seven months after the data breach.

“It’s laughable, it’s beneath contempt,” said patient Del Murphy.

Murphy is a longtime former software assurance expert for NASA and no stranger to the world of hacking.

“I’m a data expert,” he said. “I know what can happen and the seriousness of it and frankly, it scared the hell out of me.”

Gastroenterology Consultants said the company did notify federal authorities at the U.S. Department of Health and Human Services on March 19, and also preliminarily notified patients of the incident by posting a notice on its website. But neither Wietlispach nor Murphy said they had any reason to regularly check the website. Murphy said he repeatedly called the company and its Los Angeles-based law firm asking why it took months to get a letter in the mail.

“Well, we took us a while to find your address,” Murphy said he was told.

“Doesn’t take very long to find my address if I forget to pay my bill,” he said.

Privacy Rights Clearinghouse, a consumer advocacy non-profit, said timely notification is critical and hoped the Texas Attorney General’s office would take strong enforcement measures.

“Every single second that you are not aware of that breach, it’s increasing the risk of identify theft,” policy counsel Emery Roane said.

“You are unable to make the best-informed decision about whether to freeze your credit or get identify protection services.”

Gastroenterology Consultants said it provided complimentary credit monitoring and identity theft restoration services only to the small number

of patients whose social security numbers were impacted. It did not comment on why it took months to notify state authorities but said it's revised its policies and procedures to mitigate the risk of future issues.

“Gastroenterology sincerely regrets any inconvenience or concern that this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control, the company statement said.