## Quantum Computers No Threat to Encryption Yet

Fujitsu, an information and communication technology company, **conducted trials** this month to assess the difficulty for quantum computers to crack existing RSA cryptography. Using their 39-qubit quantum simulator and Shor's algorithm, they determined that a fault-tolerant quantum computer with a scale of approximately 10,000 qubits and 2.23 trillion quantum gates would be required to crack RSA. Additionally, it would take 104 days for RSA to be cracked. The most current quantum computer, produced by IBM, has 433-qubits. IBM has promised to deliver a **4,158-qubit system by 2025**.

## FinCEN Order Against Crypto Platform

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) **issued an order** that identifies the virtual currency exchange Bitzlato Limited (Bitzlato) as a "primary money laundering concern" in connection with Russian illicit finance. This is the first order issued pursuant to section 9714(a) of the Combating Russian Money Laundering Act, highlighting the serious threat business operations that facilitate and support Russian illicit finance pose to US national security and the integrity of the US financial sector. The FBI arrested Bitzlato founder Anatoly Legkodymov on 17 January in Miami. In an **additional order** published on 18 January, FinCEN noted that Binance was among the "top three receiving counterparties" of Bitzlato in terms of Bitcoin transactions.

## GoTo Suffers Data Breach with Customer's Backups Compromised

On 23 January, LastPass's parent company **GoTo provided an update** to their security incident that was disclosed in November 2022. Threat actors were able to exfiltrate encrypted backups from a third-party cloud storage service, along with an encryption key for a portion of the backups. The information that was affected may include account usernames, salted and hashed passwords, a portion of MFA settings, and some product settings and licensing information.

The GoTo products which were affected include: Central, Pro, join.me, Hamachi, and RemotelyAnywhere. MFA settings of a small subset of customers for their products Rescue and GoToMyPC may have also been impacted. Affected customers are being contacted and, out of an abundance of caution, they are resetting passwords of affected users and reauthorizing MFA settings. Additionally, affected customer accounts will be placed on an enhanced Identity Management Platform.

## 2023-24 FS-ISAC Women in Cyber Scholarship

The Financial Services - Information Sharing and Analysis Center (FS-ISAC) provides the Women in Cyber Scholarship to support women in the cybersecurity field of studies and is open to women pursuing cybersecurity degrees, enrolled in an accredited post - secondary, graduate or training program for the academic 2023-24 year. Eligible applicants must have at least one year of study remaining at the time of application and will not be eligible to graduate prior to Spring 2024. For more information, please visit the **FS-ISAC website** for more information.