21763

WORKERS
CREDIT UNION

To: NCUA, Office of Consumer Affairs and Business Regulation, and Office of Attorney General

From: Johan Seo SVP, Chief Risk Officer

Date: 07/08/2021

Subject: **Information Security Incident: Kaseya VSA Ransomware Attack (a.k.a., REvil Hacker Attack)**

To Whom It May Concern,

The following information is to provide details of the limited impact to Workers Federal Credit Union ("Workers") related to the Kaseya VSA Ransomware Attack on July 7, 2021.

The information below will also be provided to all appropriate law enforcement and regulatory agencies in compliance with all laws and regulations.

1. Detailed description of the of the nature and circumstances of the breach of security:

- On Friday July 2, 2021, Workers received an email from CISA (Cybersecurity and Infrastructure Security Agency) alerting companies to shut down Kaseya servers because of a possible ransomware attack.
    - No steps were taken at that time since Workers does not use Kaseya Software in our data center.
- On Monday July 5, 2021, Workers received an email from Avtex, our third-party call center phone system solutions provider, stating that the Avtex Servers on Workers premise were affected by the Kaseya Ransomware Attack. As a result, Workers phone system files were encrypted.
    - Workers immediately shut down these servers.
    - That evening, Workers restored the system to previous Thursday night's backup data and were up and operational by Tuesday morning.
- On Tuesday July 6, 2021, Workers conducted additional meetings with Avtex's technical support and VP of cybersecurity. Avtex hired an independent third-party cybersecurity company to assist them with determining what happened and the extent of the attack.
- At this time, there is no indication that the ransomware has retrieved any of Avtex clients' data, including Workers data. Additionally, Workers data files are encrypted as a best practice so when the ransomware encrypted our files, they encrypted already encrypted files and had no access to the keys to unencrypt them. Therefore, we do not believe that Workers members are affected since no personal information was accessed or stolen.
- We will provide any additional update if the facts of this matter materially change.

2. **The number of Massachusetts residents affected as of the time of notification:**

   - None

3. **Steps already take relative to the incident:**

   - Infected servers were shut down and new servers were created from a clean backup.

4. **Any steps intended to be taken relative to the incident subsequent to notification:**

   - Workers will continue to communicate with Avtex as they learn more from their security experts and how they will be preventing something like this happening in the future.

5. **Information regarding whether law enforcement is engaged investigating the incident:**

   - Avtex has provided notification to all relevant federal law enforcement agencies related to this matter.

Thank you.

Johan Seo,
SVP, Chief Risk Officer
119 Russell Street, Littleton, MA 01460
978-353-7084 978-501-2218 JSeo@wcu.com

WORKERS
CREDIT UNION