United Actuarial Services, Inc.
Actuaries and Consultants

2022-34

May 31, 2022

BENEFIT NEWS BRIEF

Recent Cyberattacks on Benefit Plan Service Providers

Cybersecurity has been in the news more frequently since the DOL's release of cybersecurity guidance for *ERISA*-covered benefit plans. That guidance addressed: (1) Cybersecurity Program Best Practices, (2) Tips for Hiring a Service Provider with Strong Security Practices and (3) Online Security Tips. The need for heightened cybersecurity by *ERISA* plans and their service providers was highlighted by several high-profile data security incidents that have been in the news recently.

The increasing number of cyberattacks should come as no surprise given some studies indicate that cybercriminals more than doubled the number of ransomware attacks and extortion bids in 2021 compared to 2020. That number is only expected to grow in this increasing hostile cyber environment.

We are going to take a look at four recent cyber incidents in the news and then provide some resources to prepare against cyberattacks and what to do if your plan or service provider suffers a ransomware or other cyberattack. The *HIPAA* cybersecurity guidance on cyberattacks provided by the Office of Civil Rights (OCR) discusses steps an entity must take when evaluating whether a ransomware attack is a "breach" under the *HIPAA* Privacy Rules. While OCR guidance is aimed specifically at *HIPAA*-covered entities, it is instructive for pension plans as well.

The four cyber incidents in the news that we will take a look at include: (1) Horizon Actuarial Services, (2) CaptureRx, (3) WPAS and (4) Express Scripts.

Horizon Actuarial Services Data Incident

Horizon Actuarial is a consulting firm that specializes in providing actuarial services to multiemployer benefit plans. They serve over 120 pension and health and welfare plans in various industries, including construction, trucking, professional sports, hospitality, entertainment, retail food and communication.

According to the Horizon Actuarial Notice of Data Incident, on November 12, 2021, Horizon Actuarial received an email from a group claiming to have stolen copies of personal data from its computer servers. During the course of the investigation, Horizon Actuarial negotiated with and paid the group in exchange for an agreement that they would delete and not distribute or otherwise misuse the stolen information. An investigation revealed that two Horizon Actuarial computer servers were accessed without authorization for a limited period on November 10 and 11, 2021. The

Prepared by Mike Ewing, J.D.
Director of Research
United Actuarial Services, Inc.
(317) 580-8659 • Fax (317) 580-8651
email: *mewing@unitedactuarial.com*

information accessed may have included names, dates of birth, Social Security numbers and health plan information.

Horizon Actuarial provided notice of the incident to the plans impacted by this event beginning on January 13, 2022. Beginning on March 9, 2022, Horizon Actuarial began mailing letters to individuals associated with the plans that authorized them to do so. According to the Notice of Data Incident, the data of over 50 plans was affected, including the Major League Baseball Players Benefit Plan and National Hockey League Players Association Health and Benefits Fund. The Notice of Data Incident contains a list of all impacted multiemployer benefit plans.

Two class action lawsuits have been filed against Horizon Actuarial regarding the data incident, one in the U.S. District Court in the District of Maryland and the other in the Northern District of Atlanta.

CaptureRx Data Incident

According to various sources, CaptureRx provides third-party administrative services to the healthcare industry. CaptureRx was hit with a ransomware attack that exposed the records of 2.42 million patients at multiple healthcare organizations including a hospital in New York, a community health center in Texas and a pharmacy chain in the Midwest. CaptureRx released a Notice of Data Incident about the event.

News reports indicate that in February 2021, CaptureRx was the victim of a ransomware attack at multiple locations. The files included patient names, dates of birth and prescription details. In the aftermath, a class-action lawsuit was filed against CaptureRx in July 2021 in the U.S. District Court for the Western District of Texas, claiming the company was negligent in protecting patients' information.

On February 11, 2022, CaptureRx proposed a $4.75 million settlement to resolve the class-action lawsuit. Under the proposed settlement, each plaintiff will receive about $2,000, if the settlement is approved.

Welfare & Pension Administration Service Data Incident

Welfare & Pension Administration Service, Inc. (WPAS) is a third-party administrator to over 80 Taft-Hartley and Public Trust Funds. WPAS reported that it was the target of a malware attack, resulting in the names, addresses and Social Security numbers of as many as 211,822 people potentially being compromised.

According to WPAS, on July 21, 2021, it learned that some of its computers were infected with a malware program that encrypted the affected systems. WPAS conducted an internal investigation and on July 28, 2021, the company confirmed that certain folders may have been accessed or removed from the WPAS network.

Although the company was unable to determine which files were actually accessed, it reviewed all information contained in the compromised folders and confirmed on December 20, 2021, that the names, addresses and Social Security numbers of certain individuals were included in the files. However, WPAS stated that there was no indication that specific information was accessed or misused. WPAS stated it notified potentially impacted individuals out of an abundance of caution.

Although numerous class action firms have information posted about the WPAS incident, we did not find mention of any lawsuits filed yet.

Express Scripts Data Incident

Express Scripts, a major pharmacy benefit manager (PBM), identified a credential stuffing attack on April 30, 2022 in which user IDs and passwords which had been compromised from breaches of other entities were used by bad actors against the Express Scripts member mobile application. The perpetrators were able to successfully use passwords and user IDs from these other cyberattacks because many people use the same IDs and passwords across many or all of their online accounts. The security incident involved less than 500 individuals according to Express Scripts.

The possible data points accessed included the member's name, medication name, prescription number, dosage, pharmacy name, prescriber name and prescriber contact information. Express Scripts indicated that no Social Security numbers or credit card data was compromised.

Express Scripts locked the impacted members' account to prevent any further access, and the members will be required to reset their password. Additional monitoring, blocking and preventative controls were implemented to detect and respond to malicious activity. We are not aware of any lawsuits over the incident.

Action Item

These are just a few of the recent service provider data incidents that have affected multiemployer benefit plans. In light of the increasing cybersecurity dangers, multiemployer benefit plans and their service providers need to review their cybersecurity procedures and protections against such cyberattacks. While *HIPAA*-covered entities must report breaches of protected health information (PHI), there are no similar federal rules requiring pension plans and other non-*HIPAA*-covered entities to report data breaches, an absence some say should be remedied.

Resources

Below are some resources on cybersecurity and cyberattacks. Even though the resources from OCR are specifically addressed to *HIPAA*-covered entities (health plans and business associates), much of the information would be helpful to any entity that suffers a cyberattack.

A Quick-Response Checklist from the HHS, Office for Civil Rights (OCR)
This checklist explains the steps a *HIPAA*-covered entity or its business associate should take in response to a cyber-related security incident.

12 Steps to Take Before and During a Data Breach
This informative article from the International Foundation of Employee Benefit Plans (IFEBP) was recently posted online.

OCR Fact Sheet on Ransomware

This document describes ransomware attack prevention and recovery from a healthcare sector perspective, including how *HIPAA*-covered entities and business associates can prevent and recover from ransomware attacks, and how *HIPAA* breach notification processes should be managed in response to a ransomware attack. The Fact Sheet has eight informative Questions and Answers:

1. What is ransomware?

2. Can *HIPAA* compliance help covered entities and business associates prevent infections of malware, including ransomware?

3. Can *HIPAA* compliance help covered entities and business associates recover from infections of malware, including ransomware?

4. How can covered entities or business associates detect if their computer systems are infected with ransomware?

5. What should covered entities or business associates do if their computer systems are infected with ransomware?

6. Is it a *HIPAA* breach if ransomware infects a covered entity's or business associate's computer system?

7. How can covered entities or business associates demonstrate "…that there is a low probability that the PHI has been compromised" such that breach notification would not be required?

8. Is it a reportable breach if the ePHI encrypted by the ransomware was already encrypted to comply with *HIPAA*?

Interested parties can sign up for OCR cybersecurity newsletters "*here.*"

* * *