3-USA Today-IRS

Milwaukee Bucks the victims of serious financial security breach

Matt Velazquez

Milwaukee Journal Sentinel

The Milwaukee Bucks were the victims of a serious security breach in which players' 2015 Internal Revenue Service W-2 information, including their names, addresses, Social Security numbers, compensation figures and dates of birth were disclosed to an unknown party.

The story was first reported by Shams Charania of The Vertical on Thursday and confirmed in a statement by the franchise later in the day.

On April 26 an unknown party requested the documents from the Bucks via email, using a spoof email address to impersonate Peter Feigin, the team's president. An employee responded to that email request, not knowing that it was from a fraudulent source, and provided the documents, according to the team statement.

The Bucks became aware of the incident on Monday and according to Charania sent a message to players on Wednesday night. The Bucks have already contacted the NBA and NBA Players Association as well as the relevant government agencies.

"We take this incident, and the privacy and security of our employees, very seriously," the team said in the statement released Thursday afternoon. "We immediately launched an investigation *[Legal Action]*, which is aggressive and ongoing. We quickly notified impacted individuals and are arranging for these individuals to have access to three years of credit monitoring and non-expiring identity restoration services.

"We have reported this incident to the IRS and the FBI, and will work with the authorities to continue our investigation and response to this incident.

We believe this incident arose as a result of human error, and are providing additional privacy training to our staff and implementing additional preventative measures."

Bucks officials did not wish to comment beyond the statement released by the team. Two agents for Bucks players did not respond to calls made to them Thursday.

According to Charania, player representatives with affected clients are pursuing more information about how their clients' finances and identities will be protected.

"The communication received on this major security breach is unacceptable *[Anger]*," one agent with a client on the Bucks told The Vertical. "The players need to know the exact measures being taken by the Bucks and the FBI to ensure each and every player's identity and financial information will not be compromised *[Anger]*.

"There needs to be accountability for such a mistake, details on the steps taken to rectify it and a process put in place to make sure this never happens again."

[Anger]

It is uncertain how many individuals in the Bucks organization were affected by the security breach, but the data released was not limited to players, a source confirmed.

CSO Online, a website tracking corporate cyber security, reported that more than 40 businesses were victimized by Phishing attacks targeting employee tax records in the first quarter of 2016.

On March 1, the IRS issued an alert to payroll and human resources professionals about the growing trend of BEC (Business Email Compromise Correspondence) attacks taking place online.

[Rebuild]

The form of attacks often come in the form of spoofing the email address of the company CEO or person of authority, causing the employee receiving the message to hesitate when denying the request.

One way to combat it, according to the CSO Online report, is to require verification from a second person or to include an IT or security team on any such requests, particularly when coming via email.

Charles Gardner contributed to this report. Velazquez and Gardner write for the Milwaukee Journal Sentinel, part of the USA TODAY NETWORK.