Stay Current

PAUL HASTINGS

May 2025

Follow us on LinkedIn

Compliance Update

NFL Draft Provides Wake-Up Call on Protecting Confidential Information While Working Remotely

By Daniel Prince and Chris Jalian

Last week's NFL draft highlighted more than the accomplishments of athletes at the combine or on the field. While there was extensive coverage of the merits of each player, one of the major headlines coming out of the draft involved an incident in which a coach's son accessed confidential information using his father's computer to prank call an athlete. The NFL acted quickly, committing to review "all protocols" to ensure that a similar breach does not happen again. But this should be a wake-up call for other organizations to analyze their protocols and practices related to the protection of confidential information during the course of remote work.

The Incident

Completed over seven rounds, the NFL draft is one of the most exciting television events of the year. After spending years in the weight room and on the practice field, athletes travel from across the country to attend the draft or gather with their families, waiting to be selected by one of the NFL's 32 teams.

This year, the draft status of Shedeur Sanders, the former quarterback at the University of Colorado and son of Hall of Fame player (and head football coach at Colorado) Deion Sanders, occupied the headlines for days. During the draft, Jax Ulbrich, son of the Atlanta Falcons's defensive coordinator, Jeff Ulbrich, "unintentionally came across" a draft contact number (and potentially other information) related to Sanders that was contained on an "open iPad" at his parent's home. Jax Ulbrich used the contact information to prank call Sanders by impersonating the general manager of an NFL franchise that, according to analysts, may have had an interest in drafting Sanders. The Falcons claimed that Jeff Ulbrich was "unaware of the data exposure" and committed to "cooperat[ing] fully with any inquiries" received from the NFL related to the event, including a wholesale review of its protocols.

On April 30, the NFL fined the Atlanta Falcons ($250,000) and Jeff Ulbrich ($100,000) for "failing to prevent the disclosure of confidential information[.]"Jeff Ulbrich and Jax Ulbrich also issued public apologies.

Addressing the Risks Posed by Remote Work

The incident serves as a reminder to all organizations, not only those within the NFL community, of the risks associated with remote work — namely, the unauthorized access of confidential information by third parties — and the importance of revisiting policies and practices related to the protection of confidential information. Many companies, as we emerged from COVID-19 and work-from-home mandates, have developed their technology infrastructures and tools pertaining to the data security.

But while significant investments have been made to counter the risk of unsecure networks and the use of personal accounts or devices to transmit confidential information, more work may be needed. Indeed, best practices often include:

- Training and guidance related to remote work to protect confidential information. This should include appropriate usage of work devices, company networks, electronic storage devices, etc., and restricting access to such devices while not in use.
- Analyzing policies related to device usage and monitoring.
- Entering into remote work agreements with employees requiring the safeguarding of confidential information.
- Conducting a risk assessment related to employee devices most often used to access confidential information.
- Installing technical solutions, including multifactor authentication, to "hibernate" devices after a certain interval and requiring a password to log in again.
- Exploring whether there are heightened requirements for the protection of confidential information (e.g., HIPAA, CPRA, etc.), and what controls may need to be put in place to address risks, including, nondisclosure/confidentiality agreements to further safeguard confidential information.
- Providing clear guidance on the destruction of materials containing confidential information, and tailoring policies to location/region, as appropriate.
- Reminding employees of their legal obligations to safeguard confidential information and championing a culture of compliance throughout the organization.

We have deep experience working with companies on compliance matters, sensitive investigations and remediation. We will continue to closely monitor these developments, and if you have any questions, please do not hesitate to contact the authors of this article.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact either of the following Paul Hastings Los Angeles lawyers:

Los Angeles

Daniel Prince
+1-213-683-6169
danielprince@paulhastings.com

Chris A. Jalian
+1-213-683-6143
chrisjalian@paulhastings.com