Vulnerabilities In Federal Court's E-Filing System Serves As Stark Data Security Warning For Employers

Insights
1.08.21

Overshadowed by the dramatic events in Washington, D.C. on Wednesday was the news that the electronic filing and case management system used in federal courts across the country may have been compromised by a serious security breach – serious enough that users have been advised to avoid submitting "highly sensitive" documents through the digital service. The Administrative Office of the U.S. Courts (AO) announced on January 6 that it is working with the Department of Homeland Security (DHS) to perform a security audit to identify a potential compromise to its Case Management/Electronic Case Files system (CM/ECF). What do employers need to know about this possible breach – and what lessons can you learn to avoid similar harm in your organization?

Businesses Remain Particularly Vulnerable To Digital Attacks

As the COVID-19 pandemic continues to rage into 2021, many workplaces remain as primarily remote work environments. The abrupt shift to remote work in 2020 gave IT departments little time to adapt and strengthen data security protocols, and malicious cybercriminals jumped at the opportunity to attack these vulnerable networks.

According to cybersecurity experts, cyberattacks increased by 40% to 199.7 million cases globally in the third quarter of 2020. This amounts to a 139% year-over-year increase. As we covered here, the healthcare industry remains particularly susceptible to such attacks as hospitals and healthcare providers continue to collect troves of personal identifying information during the ongoing pandemic.

Federal Courts Have Emerged As Targets

Recent events indicate federal courts are not immune to such attacks. In mid-December, the DHS's Cybersecurity and Infrastructure Security Agency issued an emergency directive regarding "a known compromise involving SolarWinds Orion products that are currently being exploited by malicious actors." In response, federal courts suspended all national and local use of the SolarWinds platform.

And then this week, the federal judiciary announced "an apparent compromise" of the CM/ECF system due to a digital cyberattack, leading to revised treatment of how parties should handle and submit "highly sensitive court documents." Each federal court is directed to issue general orders

outlining its specific filing procedures and identify which documents it considers to be "highly sensitive." Of note, the AO has stated not all documents that can otherwise be filed under seal should be considered "highly sensitive." The judiciary has announced that more guidance is forthcoming.

What Are Some Takeaways for Employers?

At this point, the most direct takeaway for businesses currently involved in federal litigation is to work closely with counsel on any pending matters to ensure documents that meet the definition of "highly sensitive" in your jurisdiction are filed outside the CM/ECF system until further guidance is released by the AO. Check for general orders issued by each court to determine the appropriate filing procedure for any such documents. The January 6 announcement indicated, for example, that federal courts will now allow highly sensitive documents to be filed in paper form or via a secure electronic device, such as a thumb drive.

The potential breach of the CM/ECF system should also serve as a reminder to employers to shore up data security protocols and educate employees on best practices for staving off cybersecurity attacks. Phishing emails have been the most commonly used tool for gaining access to sensitive company data. Phishing emails appear to be routine, work-related messages but actually contain links that, if clicked by an unsuspecting employee, could install ransomware on the employee's device. Ransomware then encrypts the company's data, which can only be unlocked with a decryption key. The cybercriminal then demands a ransom, which can range from a few hundred dollars to thousands for the decryption key.

While a modest demand may be tempting to pay in order to quickly regain access to company data, employers should take caution and seek legal advice before engaging with cybercriminals. The Department of Treasury's Office of Foreign Asset Controls (OFAC) issued an advisory opinion in October 2020 advising that companies that facilitate ransomware payments may encourage future ransomware payment demands and also risk violating OFAC regulations. As a result, companies may face civil penalties for paying ransomware demands. If confronted with a ransomware attack, companies should consider promptly contacting federal authorities for guidance, in addition to seeking legal counsel.

Conclusion

Fisher Phillips will continue to monitor the situation and provide updates as appropriate. If you have any questions regarding how cybersecurity threats could impact your organization, or best practices for addressing those threats, please consult your Fisher Phillips attorney or a member of Fisher Phillips' Privacy and Cyber Practice Group.

This Legal Alert provides an overview of a specific developing situation. It is not intended to be, and should not be construed as, legal advice for any particular fact situation.

Service Focus

Privacy and Cyber

Litigation and Trials

Counseling and Advice