Benesch

April 8, 2020

BIWEEKLY ALERT

From Benesch's **Data Privacy Defense & Response Team**

Benesch Offering Complimentary Data Privacy Defense Consultations Related to COVID-19

The global pandemic that is COVID-19 has required organizations across the world to adapt to a new reality. Companies are increasingly dependent on the internet as social distancing and shelter-in-place orders have become the norm, requiring many workforces to shift to operating on an entirely remote basis. Employees who are no longer commuting to the office are relying on their home networks to conduct even the most sensitive, confidential business.

These new changes bring with them new opportunities—FOR HACKERS!

- Hackers are capitalizing on people's desire to know what is going on, both in the world at large and within their places of employment. Scammers posing as national health authorities, such as the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC), are capitalizing on this by sending phishing and spear-phishing emails designed to trick recipients into downloading malware or providing personally identifying information (PII).
- Hackers are also creating and manipulating mobile apps designed to track the spread of COVID-19 to insert malware that will compromise users' devices and PII.
- Think your third-party video conference is secure? Maybe, but maybe not... And if you're not careful, you might get "Zoom bombed."

With the increase in activity from hackers comes an increase in activity from the plaintiff's bar. Indeed, there is already blood in the water: Last week, a plaintiff filed a class action lawsuit against Zoom in the Northern District of California, alleging that the digital video conferencing company improperly shared user data with third parties without properly notifying users. These types of a lawsuits, as well as other legal claims related to the less stringent data protection methods that can accompany a remote workforce, are only going to become more common in the coming weeks and months.

Now is the time to take action to protect your business, customers, and employees. We invite you to participate in a complimentary 30-minute call with Benesch's data protection specialists. Benesch would be happy to provide you with our insight and guidance on data protection best practices and litigation avoidance strategies. We look forward to working with you to keep your data safe and secure.

Please note that this information is current as of the date of this client bulletin, based on the available data. However, because COVID-19's status and updates related to the same are ongoing, we recommend real-time review of guidance distributed by CDC and local officials.

For more information, please contact one of the following members of Benesch's Data Privacy Defense & Response Team:

MICHAEL D. STOVSKY
Partner and Chair, Innovations, Information Technology & Intellectual Property (3iP) Practice Group; Chair, Data Security & Privacy Team; Chair, Blockchain & Smart Contracts Team
T: 216.363.4626 | mstovsky@beneschlaw.com

J. ERIK CONNOLLY
Partner and Vice Chair, Litigation Practice Group; Co-Chair, Securities Litigation Practice Group
T: 312.624.6348 | econnolly@beneschlaw.com

ALISON K. EVANS
Associate, 3iP Practice Group; Data Security & Privacy Team
T: 216.363.4168 | aevans@beneschlaw.com

WHITNEY M. JOHNSON
Associate, Litigation Practice Group
T: 628.600.2239 | wjohnson@beneschlaw.com

KATE WATSON MOSS
Associate, Litigation Practice Group
T: 312.624.6329 | kwatsonmoss@beneschlaw.com