DRI's Top 12 Information Security Recommendations for Law Firms and Other Businesses Operating in a Quarantined World

By DRI Cybersecurity and Data Privacy Committee and the **DRI Center for Law and Public Policy**
Stephen E. Reynolds, Ice Miller LLP
Barry S. Herrin, Herrin Health Law, PC
Leon Ravenna, KAR Global
Laura C. Fey, Esq., Fey LLC

We hope that all of you are feeling well and staying safe. Recognizing that many of you and your colleagues are confronting significant information security and data privacy challenges right now, the **DRI Cybersecurity and Data Privacy Committee** and the **DRI Center for Law and Public Policy** have teamed up to prepare and provide you with ***DRI's Top 12 Information Security Recommendations for Law Firms and Other Businesses Operating in a Quarantined World***.

1. **Use a Virtual Private Network (VPN):** Businesses should consider using a VPN to secure remote access to their organization's systems, documents, and contacts. If a business does not have remote VPN available, remote workers should be encouraged to assess their home network security and consider changing the password to their home internet routers. Consider limiting remote access to "trusted" devices. Consider enabling "lock, wipe, kill" technology for personal devices connecting to business platforms.

2. **Advise Employees to Confirm Home Routers are Updated:** Businesses should advise all employees working remotely to update their home routers to the current revision.

3. **Install Multi-Factor Authentication (MFA):** Businesses should consider utilizing MFA, which creates an additional authentication step on top of inputting a password, adding an extra level of security to network login or email credentials.

4. **Use Antivirus Software:** Businesses should require antivirus software on any computer accessing your infrastructure.

5. **Monitor Online Behavior and Consider Disabling Certain Access:** Businesses should enable online auditing software to make sure employees aren't navigating around the Internet unsafely. Consider disabling access to personal emails and Facebook from business-supplied technology.

DRI's Top 12 Information Security Recommendations for Law Firms and Other Businesses Operating in a Quarantined World, *cont.*

6. **Beware of Phishing Emails:** Businesses should circulate regular reminders to remote workers to stay vigilant for phishing emails and working with their information technology team to enhance their spam and phishing filters.

7. **Disable Virtual Assistants:** Employees should be required to turn off Alexa and other virtual assistants while any work-related information is being discussed—they are always listening.

8. **Securely Store and Transmit Confidential Electronic Information:** Where appropriate, businesses should consider acquiring secure cloud storage and requiring remote workers to store all confidential information on the cloud where only authorized employees are permitted access, rather than on their local machines. Remote workers should encrypt documents and email communications that contain confidential information. Alternatively, if possible, consider disabling saving to remote terminals and drives and disabling USB ports to prevent use of portable drives.

9. **Securely Store and Share Physical Copies of Confidential Information:** Remote workers should be reminded not to leave confidential information out in the open and to store such documents in a secure location. Maintain a "clean desk" policy for work at home. Any sharing of physical copies of confidential information should be handled in a secure manner. Documents with confidential information should be shredded when no longer needed. Consider disabling remote printing or printing to other than networked printers.

10. **Install Home Firewall:** If possible, executives and other employees should set up a home firewall for an extra level of security.

11. **Securely Take Confidential Phone Calls:** When conducting phone conversations, especially where confidential information will be shared or discussed, remote workers should take such calls in a private room away from other persons.

12. **Remember Physical Security:** Remote workers should always lock their devices (whether a computer or mobile device) when unattended. Remote workers should also always lock their doors when leaving their home without their devices, even for a short period of time