IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE

IN RE CBS CORPORATION LITIGATION	)	Consolidated
	)	C.A. No. 2018-0392-AGB
	)	**PUBLIC VERSION E-FILED: JULY 30, 2018**

DECLARATION PURSUANT TO 10 *DEL. C.* § 3927

Pursuant to 10 *Del. C.* § 3927, Austin P. Berglas hereby declares:

1. I am the Global Head, Cyber Forensics and Incident Response at BlueVoyant. BlueVoyant is a global cybersecurity firm that advises private sector organizations on cybersecurity risks.

2. Prior to joining the private sector, I was the Assistant Special Agent in Charge ("ASAC") of the Federal Bureau of Investigation ("FBI")'s Cyber Branch in the FBI's New York Field Office ("NYFO"), where I oversaw all national security and criminal cyber investigations in the largest cyber branch in the FBI. Overall, I was a special agent with the FBI for more than 16 years. Among other things, in my role as ASAC of the NYFO's Cyber Branch, I oversaw more than 100 employees and established the Financial Cyber Crimes Task Force, the FBI's first joint cybersecurity task force with local law enforcement. I also personally led the investigation of numerous largescale cybercrimes such as the JPMorgan Chase hack, among others. In the private sector, I have counseled

dozens of companies on ways that they can enhance their cybersecurity protections and on cybersecurity-related investigations.

3. Through my training and experience, I have become familiar with what some describe as "ephemeral messaging applications" such as Wickr and Telegram. These programs are called "ephemeral" because unlike other forms of electronic communication—such as standard email and text messaging—they are designed specifically so the messages "self-destruct" shortly after being sent or received by the users. In my experience, these applications are often used by individuals who do not wish to create a record of their communications. Specifically, in my experience as an FBI agent, I was involved in and familiar with numerous investigations where ephemeral messaging applications were used by criminal organizations such as cybercrime networks.

4. Through my training and experience, I have also become familiar with the ability to extract and reconstruct previously deleted data from electronic devices. In my career, I have overseen and supervised the extraction of data from hundreds—if not thousands—of electronic devices. In general terms, even if a user or an application deletes data from the user interface of an electronic device, fragments of the data are still often stored in what is known as a device's "slack space." While the data in the slack space is not visible to the user, it is

possible to recover this data through a combination of using electronic recovery equipment and software and manual work by trained technicians.

5. Data stored in an electronic device's slack space is not stored indefinitely, however. As a user of a device saves new information to the device—for example, by downloading or capturing new images, texts, and other files—the fragments of deleted data in the slack space is overwritten. This deletion of data in the slack space of an electronic device occurs on a continual basis, meaning the longer the user is using the electronic device to save new data the less likely it becomes that older deleted data will be able to be recovered from the device. Thus, when seeking to recover previously deleted data from an electronic device it is essential to obtain the device, or a forensic image, immediately and prevent it from data loss through usage of the device by its owner or otherwise. It is possible to try to recover deleted data from a previously made image of an electronic device, but such an image must be a full image of the device, including the slack space, as opposed to a backup of only certain files on the device. In addition, the ability to recover deleted data may differ depending on the phone model and/or operating system.

6. I understand that certain employees of CBS Corp. ("CBS") have been using an ephemeral messaging application called "TigerText." I further

understand that [redacted]

7. In my matters during 16 years as an FBI agent, and three years in private practice, during which time I have interacted with dozens of companies both large and small, I have not personally observed a single company that employed an ephemeral messaging application such as TigerText for legitimate business communications by senior executives or in-house counsel.

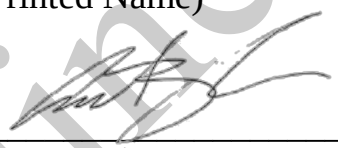
8. In my opinion, based on information provided to me to date, CBS did not deploy the TigerText application in an acceptable business use manner that would result in an enhancement to its overall cybersecurity protection. Based on publicly available information, TigerText is not an endpoint-to-endpoint encrypted messaging system. Instead, TigerText sends its messages through a third-party server hosted by the company now known as TigerConnect. In addition, per information I understand was provided by CBS, [redacted]

[redacted]

I declare under penalty of perjury under the laws of Delaware that the foregoing is true and correct.

Executed on the 23rd day of July, 2018.

Austin P. Berglas
(Printed Name)



(Signature)

CERTIFICATE OF SERVICE

I hereby certify that on July 30, 2018, the foregoing document was served electronically via *File & ServeXpress* on the following counsel of record:

David E. Ross, Esq.
Bradley R. Aronstam, Esq.
Garrett B. Moritz, Esq.
S. Michael Sirkin, Esq.
Roger S. Stronach, Esq.
ROSS ARONSTAM
& MORTIZ LLP
100 S. West Street, Suite 400
Wilmington, DE 19801

Michael Hanrahan, Esq.
Paul A. Fioravanti, Jr., Esq.
Corinne Elise Amato, Esq.
Eric J. Juray, Esq.
PRICKETT, JONES & ELLIOTT, P.A.
1310 N. King Street
Wilmington, DE 19801

/s/ Jacqueline A. Rogers
Jacqueline A. Rogers (Bar No. 5793)