C. Investigation of the Incident Uncovering the full scope of the attack took significant forensic work. We worked with and relied on experts in the field to conduct a thorough and careful investigation. In early October 2018, the investigators found on some systems evidence of malware, including MimiKatz, a tool that searches a device’s memory for usernames and passwords. Through the first two weeks of November 2018, although there was evidence of an unauthorized party on the Starwood network since July of 2014, our investigators had found no evidence that the attacker had accessed guest data in the Starwood Guest Reservation Database. On October 29, 2018, we contacted the FBI to provide them with information about the tools used by the attacker, the timeline of the intrusion, and forensic findings. Since that time, we have provided the FBI with several updates and ready access to forensic findings and information to support their investigation. At the same time, our investigative experts continued their 4 painstaking forensic work, rolling out endpoint detection technology on devices across the Starwood network. On November 13, our investigators discovered evidence that two compressed, encrypted files had been deleted from a device that they were examining. The files were encrypted and the actual content was unknown. There was also evidence to suggest that those two files had potentially been removed from the Starwood network. Six days later, on November 19, 2018, investigators were able to decrypt the files, and found that one contained an export of a table from the Starwood Guest Reservation Database containing guest data, while the other contained an export of a table holding passport information. On November 19, 2018, upon learning that the files the attacker compressed and encrypted contained personal information, we immediately began preparations to notify our guests and regulatory authorities. Recognizing that speed was of the essence, in the days that followed we worked to make sure that we could provide concrete and useful information to our guests. These efforts are described below. While these preparations were ongoing, we also began notifying regulatory authorities. On November 25 and 26, we found that, in 2015 and 2016, prior to our acquisition of Starwood, the attacker had likely created a copy of two other tables, which the attacker later deleted. The file names correspond to two other tables in the Starwood Guest Reservation Database. We have been unable to recover those files and could not determine if they had been taken. On November 29, 2018, we gave an update to the FBI and notified the four major payment card networks and their credit card processing vendors. We provided notice to regulators in over 5 twenty foreign countries and territories, as well as to state Attorneys General, the Federal Trade Commission, the Securities and Exchange Commission, and the three credit reporting agencies. II. The Scope of the Incident Our first public announcement about the incident on November 30, 2018 estimated that approximately 500 million guest records were involved, even though we knew that the numbers would likely decrease as our investigation continued and we de-duplicated the records. We issued a follow-up press release on January 4, 2019, adjusting the number of affected records downward to 383 million guest records as a result of our further investigative efforts and certain deduplication efforts. To be clear, this does not mean that information concerning 383 million unique guests was involved; in many instances, there appear to be multiple records for the same guest, but because of the nature of the data, further de-duplication cannot easily be performed. We cannot confidently determine whether records with similar names, or even identical names with different addresses, represent one person or multiple people, but we have concluded with a fair degree of certainty that information for fewer than 383 million unique guests was involved. According to our most recent investigative findings, the incident involved approximately 18.5 million encrypted passport numbers and approximately 5.25 million unencrypted passport numbers (approximately 663,000 of which have been associated with the United States). With respect to payment cards, the incident involved approximately 9.1 million encrypted payment card numbers, of which approximately 385,000 were unexpired as of September 2018. Based on our current information, we believe that the information accessed by an unauthorized third party could include several thousand unencrypted payment card numbers. To date, we have not found evidence that the master encryption keys needed to decrypt encrypted payment card and passport numbers were accessed, but we cannot rule out that possibility. Certain data analytics and 6 investigative work continues, including by a Payment Card Industry Forensic Investigator engaged on behalf of the payment card networks.