Wolverine Solutions Group (WSG)
Cybersecurity Incident
Frequently Asked Questions

Q: What happened?

A: Wolverine Solutions Group's computer system experienced a ransomware attack, which affected some of its system servers. The system had demographic data, some Social Security numbers, and clinical health information.

Q: When did the event occur?

A: WSG believes the event occurred on September 23, 2018. Shortly after that, servers and employee workstations became affected by the ransomware virus, which froze and shut down most of WSG's operations by October 2, 2018.

Q: What kind of information was exposed in this event?

A: The type of information that may have been exposed varied depending on the nature of the affected company's relationship with WSG. In some instances, the information was only demographic data (name, address, city, state, zip, and some birth dates). In other instances, some Social Security numbers and Protected Health Information were among the data on the affected server.

Q: Why wasn't I notified earlier?

A: WSG takes this situation very seriously, and WSG staff contacted and retained professional forensic experts to investigate the incident, decrypt the data, restore operations, and assess the impact to individuals, all of which was an extensive process based on the number of encrypted files at WSG. A team of forensic experts arrived on October 3, 2018 to begin the decryption and restoration process. All impacted files needed to be carefully "cleaned" of any virus remnants prior to their review by forensic investigators. Most critical programs requiring decryption were restored by October 25, 2018, and WSG's critical operations were running by November 5, 2018. However, the forensic team continued its decryption efforts on the impacted files to determine the type of information that was affected, the identities of WSG's clients and the specific individuals involved. Beginning in November and continuing in December, January, and early February, WSG discovered and was able to identify those clients whose information was impacted by the incident. The timing of notices to impacted individuals has been based on these "rolling" discovery dates. The first notices were mailed on December 28, 2018. Additional notices have been mailed in February, and further notices will be mailed in March. In addition, notice of the incident and relevant information has been posted on the websites of the various affected companies and on WSG's website (www.wolverinemail.com).

Q: What is WSG doing in response to the event?

A: WSG implemented a number of parallel steps to investigate and limit the exposure of this incident. On October 3, 2018, and over the next few days, the following actions were taken:

- *WSG notified the FBI.*
- *WSG engaged professional forensic experts.*
- *The forensic team conducted an investigation of the incident to determine what occurred and the nature of its impact.*
- *WSG and the forensic team analyzed the data that could have been affected to determine whether sensitive information had been exposed.*
- *WSG engaged a nationally recognized consultant to establish a call center to answer frequently asked questions from affected individuals.*
- *WSG is offering free credit monitoring to people who may be affected and is notifying them directly by mail about how they can sign up for credit monitoring.*

Q: What is WSG doing to prevent similar events from happening in the future?

A: WSG has:

- *Enacted policies and procedures to provide enhanced encryption at rest and in-transit, including a program that will audit the process to ensure ongoing compliance.*
- *Implemented a group of cybersecurity solutions to provide a real-time analysis of security alerts with WSG's network to maintain a secure environment.*
- *Implemented ongoing security awareness and simulated phishing programs to train and audit the WSG workforce.*

Q: Does WSG have any indication that anyone suffered identity theft as a result of this incident?

A: WSG does not know whether this information has been or will be misused. To date, the continuing and extensive reviews by a third-party forensics firm has found no evidence to confirm that there was any unauthorized access or extraction of personal data. However, it is recommended that affected members review identity theft materials posted on the Federal Trade Commission's (FTC) website at http://www.ftc.gov/idtheft. This website provides detailed information about protecting yourself from identity theft and about steps to take if it occurs. Information is also posted on WSG's website.

Q. Why did WSG have my personal data?

A. WSG performs mass printing, mailing, and other tasks for business clients, including health care providers and health plans.

Q: Is the data still in the system?

A. No. The data has been purged from the WSG IT systems.

Q: How will I know if my data was part of this?

A. You would receive a notice from us.