Q&A

Q ***Approximately how long will the three phases of recovery/testing take? Is it Days, Weeks, or Months?***

A At this time, we are unable to provide a timetable. We do know it will not be a matter of hours or days. We will routinely update the return to service status as additional information becomes available. It is important to note that we want to ensure we have resolved all issues before restarting the system in order to avoid any additional delays or inconvenience once the program is back up and running.

It is imperative that we ensure every component of the program is free from malware, thoroughly tested, and operating normally before bringing the program back online. The testing process will involve all of our agencies as well as the station owners who own and operate the computerized workstation equipment used to perform the motor vehicle inspections.

Q ***Will Applus require bank and personal information again?***

A We don't think so but will know more once we are ready to go live.

Q ***If I cancel my business checking account, what happen if APLUS tries to take money out?***

A We do not intend to withdraw funds until after the system is back up and running. At that time if ACH information has changed it can be updated then.

Q ***This is the responsibility of your company. Was our bank account information compromised?***

A Presently, we are working with computer forensics experts to determine the scope of the attack and whether any personal information may have been compromised. Unfortunately, these investigations take time. We do know that these cyberattacks are becoming more and more prevalent and affect all of us in our homes, at school, and in our workplaces.

We recommend that you monitor your financial accounts for any unauthorized activity and alert authorities and your bank if you see anything unusual. Once our investigation is complete, we will provide an update to everyone on the results of the forensic analysis.

Q ***This was the second time this month machine was down since beginning of last month, is this related to same event?***

A The two outages were not related. The first outage did not involve malware.

Q ***Is this a malware attack or is it a ransomware attack? Is this also in other countries where you do business?***

A The malware has only affected Applus in 8 US states.

Q&A

Q ***Will this affect our private networks that our workstations are connected to?***
A No.

Q ***Also should workstations be left on over the weekend?***
A Please leave the workstations on and connected to the internet at all times during the systems outage.

Q ***Will you schedule emails at a better time and not midnight so they are not lost in other emails we receive?***
A Yes.

Q ***How can we, as station owners, participate in the process to ensure all stations get reprogrammed as soon as Monday after the weekend (or when back up)?***
A Thank you for this question. We appreciate your willingness to help. We will keep you apprised as we learn more.

Q ***Would you ensure all stations treated equally by assigning an Applus representative during the restoring/testing process until stations are operational?***
A All stations will be brought online at the same time. A few may be asked to participate in Pre- Go-Live testing.

Q ***Will you notify stations once you verify if their financial information has been compromised?***
A Yes.

Q ***Has this problem affected motorcycle stickers?***
A Yes, because all systems are shut down.

Q ***The RFR for the program requires a robust business continuity plan which, among other things, includes a requirement for redundant systems. Do these systems exist and can they be activated to get the program back online?***
A They do exist but our concern is they are also affected. Our forensic team is investigating. We recommend that you monitor your financial accounts for any unauthorized activity and alert authorities and your bank if you see anything unusual. Once our investigation is complete, we will provide an update to everyone on the results of the forensic analysis.

Q ***Please provide a realistic estimate as to when vehicle inspections can resume in Massachusetts. If the answer is "unknown", please help the stations and motorists understand why.***
A As of this date, there is no timeline. Once the system is cleaned, there is a thorough testing process that will involve you as a station owner as well as the Agencies before we can safely take the system live.

Q&A

Q ***We have been told that this outage was caused by a "malware attack". Please elaborate. As part of the I/M program, each station has submitted a lot of sensitive information to Applus about their businesses and employees, including names, addresses, birthdates, license numbers, banking information, etc. Could any personal information have been stolen by bad actors? Should we be contacting our banks and changing account numbers? Has motorist information been compromised?***

A At this time, we are working with computer forensic experts to determine the scope of the attack and whether or not any personal information has been compromised. Unfortunately, these investigations take time. We recommend that you monitor your financial accounts for any unauthorized activity and alert authorities and your bank if you see anything unusual. Once our investigation is complete, we will provide an update to everyone on the results of the forensic analysis.

Q ***Ever since cameras were added to the I/M stations, the industry has raised various concerns regarding privacy and whether or not camera images could be accessed for purposes other than their intended use (i.e., who can see inside our shops when we aren't inspecting a car?). Applus' responded to these concerns by assuring the industry that only a handful of senior Applus employees had the ability to turn on cameras outside of an active inspection, and only under exceptional circumstances. In light of this network attack, is there any indication that the perpetrators have or ever had access to camera feeds?***

A We have a forensic firm analyzing the system to provide this answer. The cameras contain different credentials than other parts of the system.

Q ***Did the attack on Applus result in the infiltration of local workstations? Could there be malware on local workstations? Has Applus explored this possibility? Should station owners be concerned about the equipment in their shops? Why or why not?***

A Some workstations may have been affected which is why we intend to reimage all of them before going live. The workstations are not on the same network as the stations and we have no reason to believe it can affect other equipment not on the network.

Q ***It has been reported that this incident has resulted in the suspension of all of the I/M programs administered by Applus throughout the USA. However, the PR Newswire issued by Applus dated 3/31/2021 refers primarily to the Massachusetts program, and only mentions "other locations" in passing. Is it specifically the Massachusetts program that was attacked? Why does this press release, which can be found nationwide on scores of financial and news websites, principally refer to Massachusetts?***

A The attack has affected 8 US programs. We have notified all of those programs.

Q ***What steps is Applus planning to take to prevent future attacks after the system is returned to normal operation?***

A We have engaged computer forensic experts to assist in analyzing the current attack, restoring our IT environment to permit restoration of services, and installing additional

security measures to prevent a reoccurrence of this attack as well as anticipating and preventing future attacks that continue to evolve and adapt to those security measures. We understand the importance of ensuring the security of these transactions and the personal information attached to them and are committed to ensuring our IT environment remains secure and reliable.

Q ***How and when did Applus come to know of the attack?***

A Early Tuesday morning - March 30th, 5:27 AM Eastern.