

9.29.20

STATEMENT OF EVENTS 9.29.20 @ Approx 1130pm.

PHONE CALL FROM WYNOLHAM SUPPORT (GARY?) NEEDED TO UPDATE TERMINALS. HE ASKED IF I HAD DONE MY NIGHT AUDIT YET - I TOLD HIM NO. HE SAID IT WOULD TAKE APPROX 20 MINUTES TO DO & THAT WE WOULD START ON TERMINAL 1, I SAID I DIDN'T KNOW WHICH WAS 1 OR 2, HE SAID THE LEFT ONE WAS 1. I ASKED IF HE COULD CALL BACK SO I COULD VERIFY W/MY MANAGER IF I SHOULD ALLOW THIS OR NOT. HE SAID HE WOULD GIVE ME H.T.S NAME & EMPLOYEE # BUT WE NEEDED TO DO THIS NOW BECAUSE IT WAS THE TIME THEY HAD SCHEDULED. HE ASKED ME TO DOWNLOAD "TEAMVIEWER" & GIVE HIM ACCESS CODES. HE CALLED BACK APPROX 10 MINUTES LATER & SAID THAT IT LOOKED LIKE WE RECENTLY CHANGED OUR EMAIL PASSWORD & IF I KNEW WHAT IT WAS SO HE COULD UPDATE THAT ALSO. I GAVE IT TO HIM. I NEVER HEARD BACK FROM HIM AGAIN. AT APPROX 1230^h (9.28.20) I NOTICED THAT THERE WAS NO ACTIVITY ON THAT SCREEN SO I DECIDED TO SEE IF I HAD CONTROL - I DID. I BECAME SUSPICIOUS SO I DELETE THE "TEAMVIEWER" & "FIREFOX APPS (THAT APPEARED ON DESKTOP)". LATER IN EVENING I NOTICED THAT THERE EMAILS THAT WERE SENT BUT NOT BY US. I LOOKED AND NOTICED THAT ONE WAS A CC AUTHORIZATION THAT

WAS SENT TO US - SO THATS IS WHEN I FIGURED
WE HAD BEEN HACKED. I RELAYED EVENTS TO
OPS MANAGER + FD ATTENDANT WHEN THEY CAME IN THE
NEXT MORNING.

