**System Controls Memos**

TO: On the Spot Courier Services Management Team

FROM: That’s No Moon Software Development Team

DATE: 1 April 2019

SUBJECT: Security Measures to Prevent Possible Fraud

Our analysis of entity interactions with the system has found areas with risk of fraud. Someone could potentially pose as a customer of On the Spot to place orders as that customer. This risk could be minimized by requiring customers to create a user account with a password preventing others from placing orders under their name. Hackers could break into the system to access package status information. This could be helped by restricting access, using stronger passwords, and by encrypting communication between system components and entities outside the system. A customer could print a label intended for a one time use, multiple times, and ship multiple parcels of the same dimensions for one price. To prevent this, the system could create labels that had dates or specific codes that could only be used one time.

Unlawful characters could view a driver’s portable digital device to learn the driver’s schedule. Specifically, when deliveries are scheduled to be made and when they have been made. They could use this information to grab parcels as soon as they are dropped off, assuming the package is not signed for. Requiring customers to sign off on the delivery would ensure parcels reach the respective customer. Customers could attempt to break the payment system. One scenario as an example of this is for a customer to manipulate the system in such a way that the payment system falsely accepts payment. This could be avoided by ensuring that the system is robust and thoroughly tested before the system is deployed.

Management/administrative accounts should be protected with appropriate security measures. Possibly extra complicated passwords which could be kept secret themselves to prevent use by unlawful characters. Employees should be instructed to keep passwords secret and informed that attempts to access unauthorized accounts/information will have consequences. In addition, employees should be made aware of processes and protocols to keep the system and company protected. Management should be educated with methods to be secure with privileged information. A few examples and ideas include the following: management could be told to never leave written passwords in open areas, changing passwords frequently, logging out when finished working, using guest accounts when performing work that does not require management accounts, etc.

TO: On the Spot Courier Services Management Team

FROM: That’s No Moon Software Development Team

DATE: 1 April 2019

SUBJECT: Access Controls

Our team is going to implement access controls in the system in the near future. Access controls are defined as controls that limit a user’s ability to access resources, such as servers, files, web pages, application programs, and database tables. Access controls can include different types of authentication to restrict different types of users access to information. Our team has determined that access controls are necessary for the On the Spot because of potential security threats with customer, employee, and business information. We will be implementing customer, truck driver, and commissioner access controls.

Customer access controls will include an access control list and multi-factor authentication. The customers will not be listed on the access control list for various features or personal information on the system. Customers would need to log in with an ID and password and that would count as their multi-factor authentication. Customers would be considered registered users.

Truck driver access controls will also include an access control list and multi-factor authentication. Truck drivers would be on the access control list with the permissions of being able to view and alter sensitive information pertinent to their deliveries. Truck drivers would be required to log into the system with an ID and password as part of their multi-factor authentication. Truck drivers would be considered registered users.

Commissioner access controls will include an access control list and multi-factor authentication. Commissioners would be on the access control list and would be given permissions to everything in the system, making them privileged users. Their multi-factor authentication would include using a username and password to log into the system and challenge questions and responses.

While most individuals consider usernames and passwords to be sufficient multi-factor authentication, we believe that there are special cases that require more or different types of authentication. With the commissioner having access to every piece of the system, it is important that the system use additional methods of authentication to protect business and consumer information. The customers and truck drivers will be sufficient with username and password multi-factor authentication. If customers could make purchases with the system, we would consider adding challenge questions and responses as different methods of authentication.

TO: On the Spot Courier Services Management Team

FROM: That’s No Moon Software Development Team

DATE: 1 April 2019

SUBJECT: HTTPS Recommendation

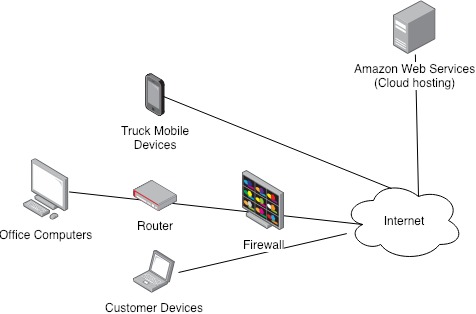
We highly recommend that you implement HTTPS on your servers. One of the many reasons being that without it, your website will show up as not being trustworthy. Information sent between the client and the server will be encrypted, causing the communication between the two to be secure. This will also help as a way that your customers can be sure that it is your website.

To implement a secure site with HTTPS you would need:

* To be a company representative
* A server with a dedicated IP address
* Business/Organization validation documents
* Correct contact information in WHOIS record
* WhoisGuard turned off

The cost to implement HTTPS would be well worth the extra security and validation it provides.

**Network Diagram**



**Network Description**

TO: On the Spot Courier Services Management Team

FROM: That’s No Moon Software Development Team

DATE: 1 April 2019

SUBJECT: Network Description and Diagram

The system is hosted on Amazon Web Services platform, which is connected to the internet. Customers and truck drivers can access the system using the internet. Office computers can connect to the internet through routers and firewalls.

Our team would like to host the system using Amazon Web Services because it provides incredible system stability and outside support. The office computers would need a router to access the internet. The firewall protects the office computers from outside threats. The mobile devices that truck drivers would use would connect to the internet to access the system.