CUSTOMER SECURITY BULLETIN
FAQ

29th October 2021

To Whom It May Concern:

Most payment service providers & acquirers around the world who work with PAX Technology know & trust our new-generation Android-based payment terminal solutions.

This comprehensive list of Frequently Asked Questions addresses recent unsubstantiated claims made in the media around perceived security concerns in PAX products.

In summary, there are no security issues.
We can confirm there has been no compromise of confidential customer or cardholder information, no data leaks, no security cracks and no loss or breach of transaction data.

Payment service providers and their merchants who use products manufactured by PAX Technology can remain fully confident of the security & reliability of our payment terminals.

Please do not hesitate to contact us for further clarification.

Yours sincerely,

Alex Dong
Vice President R&D

Simen Cai
Technical Director

1. WHAT IS THE ROOT OF CONFUSION AROUND THE SECURITY OF PAX DEVICES?

Concerns about the security of our devices appear to be rooted in a misunderstanding of our Android-based technology.

As our many long-standing customers around the world know, PAX Technology is at the forefront of developing state-of-the-art Android-based payment terminals. Android, and in particular our globally successful PAXSTORE platform, are what set PAX apart.

An Android-based operating system comes with enormous advantages, allowing PAX devices to offer many advanced features - similar to smartphone technology - such as geolocation, that are unavailable on traditional POS terminals. These enhanced features naturally involve more complex technology that require connectivity with more networks, which can lead to the misimpression that an Android-based device is less secure.

Crucially, the Android element is, of course, separate from the payment processing element within a PCI & EMV certified PAX terminal. Data that 'flows' through the payment processing engine of a PAX device never 'flows' through the Android operating system.

2. ARE THERE CONCERNS THAT DATA HAS BEEN EXPOSED?

Absolutely not. As required by the many different certifications and payment industry mandates covering our devices, all payment data and all personal information are securely separated and firewalled in PAX products. Indeed, it now appears that the acquirer in question has publicly stated there is no evidence that any information has been exposed.

Again, this is because data that 'flows' through the payment processing engine of a PAX device never 'flows' through the Android operating system.

3. WHY DID A PAYMENT PROCESSOR IN THE USA ISSUE A NOTIFICATION SAYING IT WOULD REPLACE PAX TERMINALS WITH THOSE OF VERIFONE OR INGENICO?

We are not sure, because they since confirmed, as per a report on Yahoo Finance[1], that they have not found any evidence that data running through PAX POS devices has been compromised.

As is normal in the course of business any new customer, PAX USA engaged with the payment processor's security & compliance teams in answering questions about our solutions. They asked a few very detailed questions regarding geolocation reporting and IP

[1] https://finance.yahoo.com/news/fis-worldpay-replaces-pax-terminals-175959727.html

addresses that PAX devices connect to. The response from PAX USA answered some of the questions, but apparently not to the level of detail that the payment processor was expecting. Instead of working closely with PAX USA to get better answers, their vendor risk management team sent PAX USA an email saying they decided to stop deploying PAX devices globally. They sent emails to customers that they had decided to provide merchant clients with point-of-sale devices manufactured by Verifone and Ingenico, and that they would replace all PAX devices with new devices provided by Verifone or Ingenico at no additional cost to the merchant.

Based on our exchange with the acquirer, we believe their sudden decision was likely the result of miscommunication and misunderstanding in two areas:

- The optional geolocation feature available on PAX terminals;
- The use of dynamic IP addresses, commonly also used for geolocation.

While our geolocation features and use of dynamic IP addresses are fully compliant with industry security requirements, we recognize that some people may not be familiar with these particular areas and explain them in more detail below.

4. WHAT IS GEOLOCATION?

Geolocation allows customers to pinpoint the location of their PAX device, similar to apps that allow users to find the location of their smartphones. Geolocation maps the whereabouts of devices with even more accuracy than GPS, by using technology that tracks a device even in areas where there is no GPS signal.

For this feature to function, geolocation software identifies wireless networks within range of a PAX device, and communicates the identity of wireless access points to the geolocation service provider. The geolocation service provider then uses such information to more accurately pinpoint the location of the device.

Most importantly, this is a one-way communication: the PAX device sends wireless network information to the geolocation service provider, but the geolocation service provider *cannot* communicate with the PAX device to obtain *any other* information on the terminal.

5. WHY ARE GEOLOCATION SERVICES IMPORTANT?

PAXSTORE users worldwide know that geolocation allows you to visually track & locate your PAX device on a map. If a PAX terminal is stolen, for example, geolocation lets customers know that the device is no longer in the area it should be in.

In addition to providing location data, many customers rely on this feature as an additional security measure to geofence, or ‘brick’, a device that moves outside a designated merchant location, which again in the example of a device being stolen, can include an enhanced security feature of automatically wiping all data and customer information.

6. COULD GEOLOCATION CAUSE CONFUSION ABOUT PAX DEVICE SECURITY?

Possibly. To make geolocation an available feature, PAX SmartPOS terminals utilize a third party geolocation service provider, just as your smartphone does. These services require devices to communicate geolocation information to third party IP addresses, some of which may be outside the country where devices are operational.

Again, the *only* information being provided to a geolocation service provider is information about the actual location of a PAX devices. No payment data and no customer data is *ever* transmitted to the geolocation service provider, because these are completely and securely separated, *and* firewalled, from geolocation services.

7. WHAT ARE DYNAMIC IP ADDRESSES?

Many advanced Android-based services, including geolocation, use dynamic IP addresses as do most IP based services. Dynamic IP addresses can, and will, produce changing IP addresses at any given time, and also during a ‘trace’, making it almost impossible to detail or “whitelist” every IP address.

In all cases, however, PAX devices *only* connect to known servers through these dynamic IP addresses, and all payment data and all personal information are completely and securely separated, and firewalled, from such services.

8. HOW IS PAX CONTINUING TO IMPROVE SERVICES OFFERED?

Today, there are approximately 4 million Android SmartPOS terminals connected to circa 150 independent PAXSTORE marketplaces globally, of which 65 are in the EMEA region.

The current geolocation service provider is *fully compliant* with all security protocols. Because we appreciate that certain customers may, for whatever reason, feel more comfortable utilizing a geolocation service provider located *outside* of China, PAX EMEA already announced to all PAXSTORE administrators that an alternative optional geolocation service, provided by US-based company Skyhook, is available from next month.

Customers who remain concerned about geolocation know they can easily turn off the geolocation service through their PAXSTORE account.

9. ADRESSING 6 SPECIFIC CLAIMS MADE IN THE KREBS[2] ARTICLE?

i. "*Krebs on Security heard from a trusted source that the FBI began investigating PAX after a major U.S. payment processor started asking questions about unusual network packets originating from the company's payment terminals.*"

- We presume this is the payment processor's reference to transmission of geolocation data. This is addressed above.
- Android-based SmartPOS terminals typically have multiple applications deployed, each sending relevant data to its respective host.
- Applications need to be signed by the developer and then also need to be signed with the relevant PUK key in order to be installed on a PAX device. Only approved applications can be installed. Thus, any malicious malware would need to be signed with a valid PAX PUK in order to be installed and run on the device.

ii. "*According to that source, the payment processor found that the PAX terminals were being used both as a malware "dropper" - a repository for malicious files - and as "command-and-control" locations for staging attacks and collecting information.*"

- No evidence or proof has been provided that this is true or that any malware or malicious files were indeed found on a PAX device.
- Are these references to debug device or production device? No factual information been provided to PAX.

iii. "*"FBI and MI5 are conducting an intensive investigation into PAX," the source said.*"

As of the date of this document:

- Nobody from MI5 in the UK contacted PAX or any related partners or customers.
- US law enforcement authorities have not indicated the purpose or subject matter of the investigation, nor filed any charge against any entity or individual in relation thereto. PAX will assist law enforcement authorities with any required investigation.

iv. "*A major US payment processor began asking questions about network packets originating from PAX terminals and were not given any good answers.*"

- Although the article does not refer to which type of network packets, we presume (based on prior engagement with the payment processor) that this relates to geolocation and/or IP addresses, which points 6 and 7 above address clearly.

[2] https://krebsonsecurity.com/2021/10/fbi-raids-chinese-point-of-sale-giant-pax-technology/

v. “*My sources say that there is tech proof of the way that the terminals were used in attack ops,...*”

- No factual evidence or proof has been provided to PAX. If and when received, it would, of course, be immediately investigated.

vi. “*...the source said. “The packet sizes don’t match the payment data they should be sending, nor does it correlate with telemetry these devices might display if they were updating their software.*”

- Data being sent from a point-of-sale-terminal would very much depend on the applications installed and how they are configured or how frequently they are configured to communicate with the respective host.
- Packet sizes for payment data (containing transaction specific data) would differ from that of telemetry data (which is data about the status of the device, battery usage, memory usage, CPU usage, network data usage, printer paper status, etc.) and that of software / firmware data (firmware or application package data).
- Similarly, the packet data identified relates to data being sent to a specific (geolocation or other app) service provider and would naturally be different in size from other data packets mentioned above.
- The data packets would need to be analysed in order to determine any malice and cannot be based purely on packet size.

10. ARE PAX TERMINALS SECURE AND SHOULD I CONTINUE USING THEM?

Certainly. There are no known security risks in our products of services. PAX terminals deployed by payment service providers and their merchants are PCI & EMV certified and have received many types of card scheme, contactless and other certifications.

PAX devices connect to many different acquiring banks & payment processors around the world, through many payment software applications, each of which are certified and approved to country-level and/or acquirer-level standards.

The IT & Security departments of such payment service providers and acquiring banks are aware that part of their responsibility lies in ensuring that the terminal estates they have deployed into the field are kept up to date in terms of software, thus guaranteeing transactional security for the merchants they serve.

Furthermore, PAX terminals and software apps combined have been thoroughly tested by our customers, and any 3rd party security companies engaged by them, and have stood the test of time in terms of security & reliability when deployed in the field.