Application of Regulation 2023/1542[1] to Point-of-Sale hardware

Payments industry call for clarification

12 April 2024

Summary: The digital payments industry urges the European Commission to clarify and confirm the exclusion of point-of-sale ("POS") hardware from the requirements laid down in Article 11(1) of the new EU Regulation 2023/1542 on Batteries and Waste Batteries ('the Regulation").

Art. 11.1 of the Regulation requires that electronic devices must have batteries that are "*readily removable and replaceable by the end-user at any time during the lifetime of the product*". This needs to be possible without "*specialised tools*" and applies to whole batteries.

The digital payments industry considers that the replaceability and removability obligations shall not apply to POS hardware as they meet both the criteria under Article 11.3, namely, it requires a continuous power supply to "*ensure the safety of the user and the appliance*" and for "*data integrity reasons*".

User and Appliance Safety Considerations

- Lithium-ion batteries - commonly used in POS hardware due to their high-performance standard and longer life than other battery forms - pose inherent safety risks such as overheating, sparking, and fire when mishandled or punctured. **Allowing end-users (merchants) to remove and replace these batteries could inadvertently lead to hazardous conditions**. Mishandling scenarios, such as exposure to high temperatures or physical damage, are common and likely when not carried out by trained technicians, thus necessitating a permanent connection between the product and the respective battery for user safety.
- Many POS devices are subject to water or other liquid exposure in wet environments like bars, restaurants, and outside venues. Allowing merchants to replace batteries and creating a more porous device runs a **higher risk of water going into the device and the device malfunctioning.** Moreover, increased vulnerability to liquids may increase the number of POS devices unnecessarily replaced, with material impact on electronic waste and increased costs for merchants.

[1] Regulation (EU) 2023/1542 of the European Parliament and of the Council of 12 July 2023 concerning batteries and waste batteries, amending Directive 2008/98/EC and Regulation (EU) 2019/1020 and repealing Directive 2006/66/EC

Data Integrity Considerations

- POS devices are meticulously designed to detect and respond to attempts to access internal elements, in compliance with existing Payment Card Industry Data Security Standards ("PCI DSS"). The PCI DSS are established industry-wide security standards for protecting payments data. Compliance with these standards is critical to safeguard sensitive financial information and is a requirement for any manufacturer and distributor of POS devices.
- Compliance with industry standards necessitates stringent penetration testing as per the PCI PIN Transaction Security (PTS) and Point of Interaction (POI) Modular Security Requirements. Penetration testing ensures that bad actors are not able to tamper with the device in ways that could compromise payments data. This testing process begins by examining the outer casing of the device so by adding additional ways to access the device, such as for battery replacement, this would make the device less secure and more vulnerable to hackers trying to steal payment data.
- Specifically, A1 - and most of "Section A" of Physical Security Requirements of PCI PTS referenced above (page 13 and onwards) - can only be met by designing POS devices with **robust tamper-detection circuitry, which is maintained by ensuring continuous power supply and is therefore an integral part of many POS battery architecture designs**. This tamper-detection circuitry ensures that POS devices are engineered to respond to any attempts to open the device as a potential intrusion by erasing cryptographic keys and sensitive data. This preventive measure maintains data integrity and safeguards both merchants and customers by ensuring that sensitive data is irreversibly erased before it can be accessed.
- This tamper-detection circuitry also protects POS devices from fraudulent attacks without user awareness, such as the insertion of credit card skimmers, by preventing access to cryptographic keys or sensitive data.
- Not having a continuous power supply to a tamper circuit would result in **non-compliance with PCI DSS and PCI PTS requirement**s. As a result, this **would prevent POS hardware from being put on the market and could entail serious penalties, loss of trust, and financial repercussions for merchants and consumers alike.**

Based on the above, given the importance of continuous power supply for user/appliance safety and data integrity, we believe that Article 11(3) exemption applies to POS hardware.

Finally, whilst we recognise the importance of extending the life of hardware to reduce waste and enhance sustainability, we note that the lifespan of POS hardware is hardly dependent on battery life duration. Factors like demand for increased processing power, memory, storage and better performance, along with fast technological advancements - such as AI and software developments - greatly influence POS devices' duration.

* * *

We, the undersigned trade bodies, **urge the European Commission to confirm our understanding that the replaceability and removability battery requirements set out in Article 11.1 of the Regulation do not apply to POS hardware**. By clarifying POS hardware is not mandated to comply with these obligations, the European digital payments industry can continue to uphold the integrity and security of payment transactions for consumers and businesses across the EU.

We remain committed to working collaboratively towards sustainable solutions that balance environmental objectives with the unique challenges faced by the payments industry.