P2PE Implementation Manual

Thumbzup Innovations (Pty) Ltd
cnr Von Willich Ave & Leonie Str
Ground Floor, Building A, Trent Bridge Office Park
Centurion
0157

Document Control

Title	P2PE Implementation Manual
Document Number	WD-THB-160
Document Version	1.5
Publish Date	October 5, 2019 at 02:21:05 PM
Current Status	Approved
Confidentiality Level	Public

Revision History

Date	Version	Author	Change notes
2017 04 11	0.1	Derek Keats	Initial version
2017 05 02	0.2	Colet Smit	Input from Colet
2017 05 12	0.3	Derek Keats	Added new section
2017 05 19	0.4	Derek Keats	Further editing, improvements, PIN entry added
2017 06 01	0.5	Derek Keats	Minor edits
2017 06 01	0.6	Derek Keats	Corrections after feedback received
2017 06 21	0.7	Derek Keats	Corrected spelling error, removed section numbering for “Overview
2017 10 18	0.8	Derek Keats	Changed contact info to me temporarily until we have employed account manager to avoid conflict of interest with key custodian
2017 10 19	0.9	Derek Keats	Reverted the change as it was a misunderstanding
2017 11 10	0.10	Derek Keats	Fixed name of the company and version of firmware not matching PICSSC website
2017 12 15	1.1	Derek Keats	Removed reference to wrong firmware version
2018 01 31	1.2	Derek Keats	Added firmware versions 3.0.14 and 3.1.2 to supported firmware
2018 02 01	1.3	Derek Keats	Inserted section 5.4
2018 11 28	1.4	Albert Mbaimbai	Change Company address, Added Solution ref number Per SSC website Added hardware version P5.0.2.X Added firmware versions 3.0.13,3.0.15,3.1.3,3.1.4,3.1.5 and 3.1.7 Typo correction at Section 3.3
2019 02 05	1.5	Colet Smit	Section 2.2: Contact Information Section 4.1.1: Receiving of a device Section 5.2: List of trusted sites Section 6.2: Contact Number Table 2 – Correction of Type Section 9.3: Device activation and deactivation

Document Approval

Date	Version	Approval Description / References
2017 06 01	0.5	Approval of P2PE Implementation Manual for Thumbzup solutions WD-THB-160 v0.5
2017 06 21	0.7	Approval of P2PE Implementation Manual for Thumbzup solutions WD-THB-160 v0.7
2017 02 25	1.3	Approval of P2PE Implementation Manual for Thumbzup solutions WD-THB-160 v1.3
2018 11 28	1.4	https://jira.thumbzup.com/browse/DOC-127
2019 02 05	1.5	https://jira.thumbzup.com/browse/DOC-155

Table of Contents

1. Overview

This document provides guidelines for merchants implementing the Thumbzup Payment Pebble® version tCR2 either as a bring-your-own-device solution, or as part of the Thumbzup Payment Blade.

Figure 1 : Payment Pebble® version tCR2 as a bring-your-own-device solution (left), and as part of the Thumbzup Payment Blade (right)

While the main focus of P2PE is the Payment Blade implementation, the same certification is available to smaller merchants whether they use the Payment Blade or the Payment Pebble® tCR2as part of a bring-your-own-device solution.

The terms “Payment Pebble®” and “card reader” are equivalent.

2. P2PE Solution Information and Solution Provider Contact Details

2.1. P2PE Solution Information

Solution name:	Thumbzup Payment Pebble solution
Solution reference number per PCI SSC website:	2017-00969.001

2.2. Solution Provider Contact Information

Company Name:	Thumbzup Innovations (Pty) Ltd
Company address:	Building A, Trent Bridge Office Park cnr Leonie str & Von Willich Ave Doringkloof Centurion 0157 South Africa
Company URL:	http://www.thumbzup.com
Contact name:	Thumbzup Helpdesk
Contact phone number:	+27 87 550 2687
Contact e-mail address:	security.sa@thumbzup.com

2.3. Returning POI devices to Thumbzup

Devices should be returned via courier to Thumbzup. Thumbzup should be alerted that a device is being returned, including the reason, by sending an email to returns@thumbzup.com

Company address:	Building A, Trent Bridge Office Park cnr Leonie str & Von Willich Ave Doringkloof Centurion 0157 South Africa

---

P2PE and PCI DSS
Merchants using this Thumbzup P2PE Solution may be required to validate PCI DSS compliance and should be aware of their applicable PCI DSS requirements. Merchants should contact their acquirer or payment brands to determine their PCI DSS validation requirements.

---

3. Approved POI Devices, Applications/Software, and the Merchant Inventory

3.1. POI Device Details

The following information lists the details of the PCI-approved POI devices approved for use in this P2PE solution. Note all POI device information can be verified by visiting the website: https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

POI device vendor:	Thumbzup UK Limited
POI device model name and number:	Payment Pebble® model tCR2
Hardware version #(s):	P5.0.1, P5.0.2 and P5.0.2.X
Firmware version #(s):	3.0.3, 3.0.7, 3.0.10, 3.0.12, 3.0.13, 3.0.14, 3.1.2, 3.0.15, 3.1.3, 3.1.4, 3.1.5 and 3.1.7
PCI PTS Approval #(s):	4-60203

3.2. Software / application details

The Payment Pebble® does not support the installation and running of applications on the secure device. Because the architecture separates the trusted (Payment Pebble® device) from the non-trusted (host mobile phone, tablet or Payment Blade), software is only available to run on the host. This increases security by not having any applications that are allowed to access sensitive cardholder data.

3.3. POI Inventory & Monitoring

- All POI devices (Payment Pebble® / Payment Blade with included Payment Pebble®) must be documented via inventory control and monitoring procedures, including device status (deployed, awaiting deployment, undergoing repair or otherwise not in use, or in transit).
- This inventory must be performed annually, at a minimum.
- Any variances in inventory, including missing or substituted POI devices, must be reported to Thumbzup via the contact information in Section 3.1 above.
- The inventory must be updated whenever a POI is received prior to deployment, removed for repair or waiting transport between sites locations, etc.
- Sample inventory table below is for illustrative purposes only. The actual inventory should be captured and maintained by the merchant in an external document.

Sample inventory table (actual document to be created and maintained by merchant)

Device	Model number	Device location	Device status	Pebble serial number

4. POI Device Installation Instructions

Do not connect non-approved cardholder data capture devices
The P2PE solution provided by Thumbzup is approved to include only the Payment Pebble® PCI-approved POI device. Only these devices denoted above in section 3.1 are allowed for cardholder data capture. The design of the Payment Pebble® prevents the connection of non-compliant accessory devices and non-compliant data capture mechanisms.

Do not change or attempt to change device configurations or settings.
Changing device configurations or settings is not something that is accessible to the merchant. Any tampering with the physical device will invalidate the PCI-approved P2PE solution in its entirety, and will trigger the devices to delete their keys and become non-functional. Attempting to physically open the device will cause it to delete its keys and become non-functional. You cannot install applications onto the Payment Pebble®, only onto its host phone, tablet or Payment Blade

---

4.1. Installation instructions

4.1.1. Receiving the device

Before accepting the device from the courier:

1. Check the silver seal on the box for evidence of tampering (Figure 2). If any of the seals show the word “Void” then the device should be returned in accordance with the specified procedure. Thumbzup should be alerted by email of the tampering, including the shipment information, and seal number.
2. Check that the number on the silver tamper evident seal (Refer to Figure 2) corresponds to the delivery documentation
3. Check that the device serial number (Refer to Figure 3) corresponds to the delivery documentation

If any of the above is not correct, please do not accept the device or open the box and try to transact with the device. Follow the return procedure to return your device.

4.1.2. Installation instructions

At first use the merchant is required to input the recognised merchant ID against which the device will transact, as well as provide a username. Please see the insert that is shipped with the device for instructions related to the particular configuration that you have received.

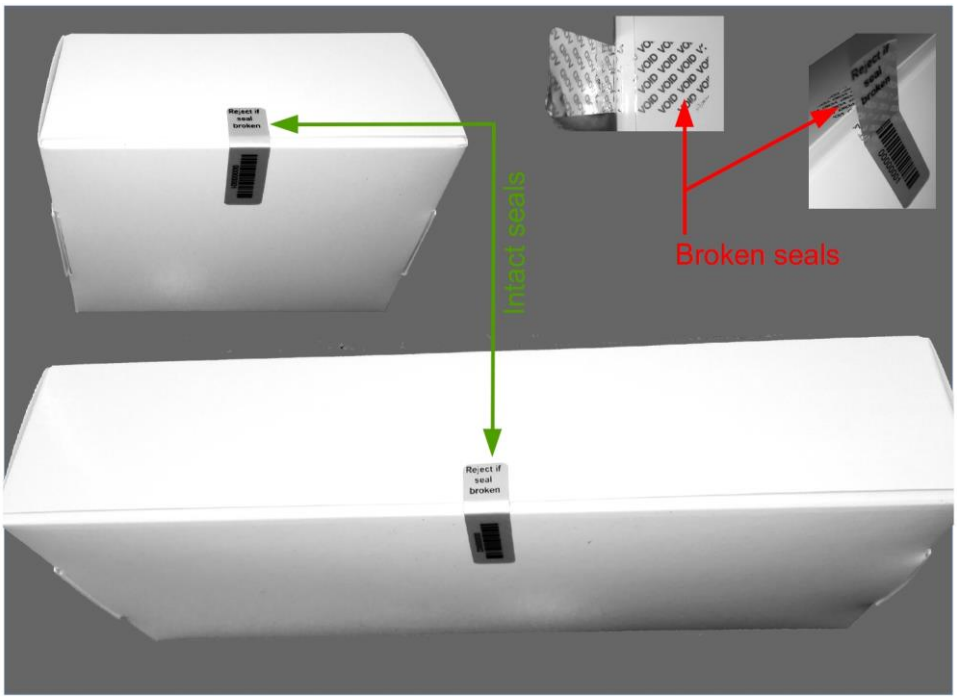

Figure 2 : Box showing tamper-evident seals. Any devices found to have tampered seals should be rejected. Note that boxes may differ in covering, and shipped boxes may include a sleeve.

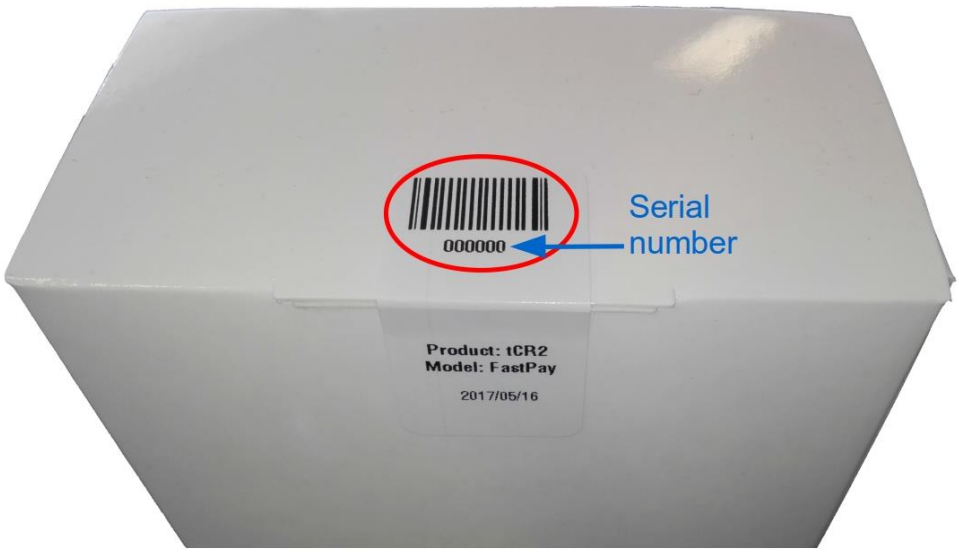

Figure 3 : View of box showing the location of the serial number.

Physically secure any POI devices in your possession, including devices:

- *awaiting deployment*
- *undergoing repair or otherwise not in use*
- *waiting transport between sites/locations.*

4.2. Guidance for selecting appropriate locations for deployed devices

The value of a payment and business mobility solution is in part due to its ability to be used in any location. In this way, the POI that forms part of this P2PE certified solution is different from a typical card-payment terminal, and security features are designed to allow more flexibility in location of use. However, the merchant is still responsible for ensuring the security of the device.

Do not allow public access to the device except during the course of processing a transaction where an individual may be required to enter their PIN. Check the devices daily to ensure that they are performing as expected.

4.3. Guidance for physically securing deployed devices to prevent unauthorized removal or substitution

The value of a payment and business mobility solution is in part due to its ability to be used in any location. In this way, the POI that forms part of this P2PE certified solution is different from a typical card-payment terminal, and security features are designed to allow more flexibility in location of use. However, the merchant is still responsible for ensuring the security of the device, for example by never allowing the device to be left unattended or unsupervised.

If the device is part of a Payment Blade, the Payment Blade is equipped with a Kensington lock that can be used to secure the Blade to a physical structure. Merchants should never allow the device to be left unattended or unsupervised. For shop floor attendants, at events, markets, and in related circumstances, it is recommended that the device be clipped to a belt or otherwise secured to a person.

When the device is not in use it should be stored in such a way as to prevent unauthorised removal or substitution. Some recommendations are:

- Secure devices in a locked room when not in use.
- Assign responsibility to specific individuals when device is in use, and sign them out for use and in for storage.
- Do not allow a device to be away from the responsible person without it being stored in a safe place.
- In retail establishments, observe the device much as you would for a normal point of sale device.

5. POI Device Transit

5.1. Instructions for securing POI devices intended for, and during, transit

Being a business mobility solution, the Payment Pebble® and Payment Blade are designed to be transported and used at remote locations. However, they should be handled in such a way as to prevent theft or handling by unauthorised personnel.

In the event that the device is shipped by a third party, the following recommendations apply:

- Shipping should be done via a trackable method (for example, private courier services or public shipping companies that provide status during shipping);
- The serial or EMI number of the device should be recorded;
- Notification should be done to the company to which the package is shipped, including package tracking details, and serial or EMI number.

5.2. Instructions for ensuring POI devices originate from, and are only shipped to, trusted sites/locations

Thumbzup Payment Pebbles® intended for use in the merchant's mobile phone or tablet or shipped together with the Payment Blade will be in a box sealed with numbered, tamper evident tape.

A manifest will be sent separately that includes the EMI number of the Blade, as well as the number on the tamper-evident seal. It is the merchant's responsibility to check that the seal has not been tampered or opened and that the EMI number corresponds to the manifest. If there are signs of tampering, or the numbers do not correspond, then the device in its box should be returned to Thumbzup in the manner indicated in section 1.3, with an explanation that the device arrived with evidence of tampering.

The location from which shipping to the merchant can be done is as follows :

- **Thumbzup Innovations**
  Building A, Trentbridge Office Park,
  cnr Leonie str & Von Willich Ave,
  Doringkloof,
  Centurion, 0157,
  South Africa

You will receive a manifest via a separate means of communication, typically by email. The devices will never arrive without meeting the criteria described above. In the event that you believe you have received a device from an untrusted source, the device should not be used unless it is verified.
Please call +27 87 550 2687 and report it.

6. POI Device Tamper Monitoring and Skimming Prevention

6.1. Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity

The merchant or acquirer must visually inspect the device for any sign of tampering when it is received. These checks should also be done on a regular basis after receipt and installation. Ideally these checks should be done before each transaction otherwise at least once each day of use.

Inspect the Payment Pebble® (which is inside the transparent casing if shipped with a Payment Blade) for any scratching, bending, or breakage in the plastic. For all other forms of tampering, the device screen will show that it is compromised.

The following are things that can be inspected:

- The tCR2 device is a sealed unit and is not designed to be opened. Check for evidence that the case has been opened. For BYOD pebbles (not visible in Payment Blade version), there is a security label at the bottom of the unit that must not be damaged.
- There are no warning messages shown on the display when switched on.
- There is no evidence of any unusual wires that have been connected to any parts of the device.
- There are no unusual holes in the device.
- There are no unexpected stickers attached to the device.
- Once configured, ensure that the correct merchant name is displayed.
- There is no shim or foreign objects in the chip card slot. The chip card slot has no joints and has no protruding objects. See Figure 4.

Should a device be tampered with, or if the device is opened, all keys are erased, and the device will not be able to process any transactions. A device that has been tampered will indicate the fault as shown in Figure 5 (SEC: Compromised). The device must be returned for inspection.

Figure 4 : Top view of a healthy, untampered Payment Pebble®.

Additional guidance for skimming prevention on POI terminals can be found in the document entitled Skimming Prevention: Best Practices for Merchants, available at www.pcisecuritystandards.org

---

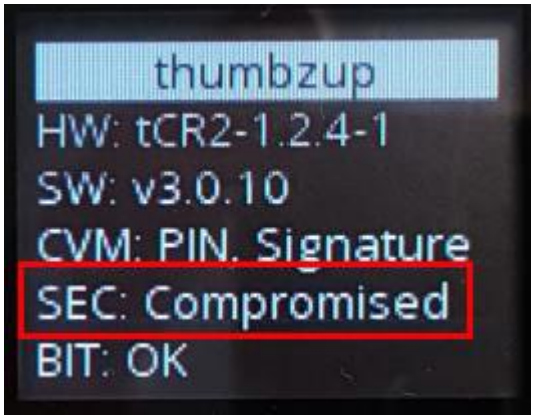

Figure 5 : Payment Pebble® screen showing a tamper condition.

6.2. Instructions for responding to evidence of POI device tampering

If you find evidence of device tampering, please contact Thumbzup security using one of the following methods:

- Email: security.sa@thumbzup.com
- Telephone: +27 87 550 2687

6.3. Instructions for confirming device and packaging were not tampered with, and for establishing secure, confirmed communications with the solution provider

Refer to Section 4.1

6.4. Instructions to confirm the business need for, and identities of, any third-party personnel claiming to be support or repair personnel, prior to granting those personnel access to POI devices

Thumbzup POI devices generally do not need third party access, but there may be support requirements to change network settings, SIM cards, or provide demonstration of use. Before allowing any third party access to the POI devices, confirm with the relevant internal stakeholder that the device being accessed has a business need for that access.

In the event that an unknown third party requests access to a device, after confirming the business need, confirm their identity using a picture ID and then contact Thumbzup to confirm that this person is officially acting on behalf of Thumbzup. In the event that the third party is acting on behalf of a reseller or support contractor, ensure that this confirmation of identity is made with the relevant entity.

7. Device Encryption Issues

7.1. Instructions for responding to POI device encryption failures

If an encryption failure happens, it will be indicated as a hardware error, no cardholder data would be in a human-accessible form. If the device refuses to transact or the mobile application indicates that it should be returned to the supplier, then the merchant has an obligation to return it for replacement.

7.2. Instructions for formally requesting of the P2PE solution provider that P2PE encryption of account data be stopped

This cannot be requested for the Payment Pebble® as there is no mechanism to stop the encryption of account data.

8. POI Device Troubleshooting

8.1. Instructions for troubleshooting a POI device

The Payment Pebble® and Payment Blade should work out of the box, provided they are given a charge cycle after unpacking. In the event that problems occur, check the list below. If none of these solve the problem, contact the Thumbzup support number.

Table 1 : POI troubleshooting instructions

Device won't switch on	Check that the device is charged. If not, charge according to the provided instructions and try again.
Incorrect Card Reader	Check that the MID is correctly entered. If it is, then contact the issuer of the MID.
Cannot contact Card Reader	Ensure that the Pebble (Card reader) is charged, and connected.
Cannot contact server Network connection failed	If using mobile network, check that the SIM card is installed correctly, and that there is a signal. If using Wi-Fi check that the password is correctly set.
Transaction timed out	The transaction did not go through. You will have to try it again. If using GSM network, try moving to a location with a better signal.
One time PIN (OTP) entered incorrectly 3 times	Contact the support number to have the PIN reset. A new OTP will be sent to your registered phone via SMS.

If there are any other issues, please contact the support number provided in Section 2.2

9. Additional Solution Provider Information

9.1. The importance of charging

Whether used with a mobile phone or tablet, or as part of the Payment Blade, the Payment Pebble® must be kept charged. If the Payment Pebble® battery is completely drained, the device will be unable to maintain its physical security functions and its cryptographic keys, which will render it inoperable.

When the battery reaches critical level, the device stops transacting and reports that the battery is critical via the mobile app on the host device. If a battery critical warning is shown, the device must be charged immediately to prevent permanent damage, and total loss of function.

9.2. PIN entry

The Payment Pebble® implements Thumbzup's unique patented secure PIN entry method that makes use of the insecure touch screen on the smart phone for the PIN entry, whilst keeping the PIN secret from the smart phone. The PIN entry method uses the secure Payment Pebble® device, and allows the cardholder who knows the card PIN to make a visual association between the two devices whilst preventing the smart phone application from ever knowing the PIN.

When the PIN is to be entered, a map of the keypad is displayed on the secure screen of the Payment Pebble® device. The layout of the keypad map shows the numeric keys in randomly reordered positions to ensure that the PIN will never be known to the smart phone. The cardholder enters a PIN by pressing the button on the smart phone screen that corresponds to the grid position of the numeral shown on the keypad map displayed on the secure screen of the Payment Pebble® device.

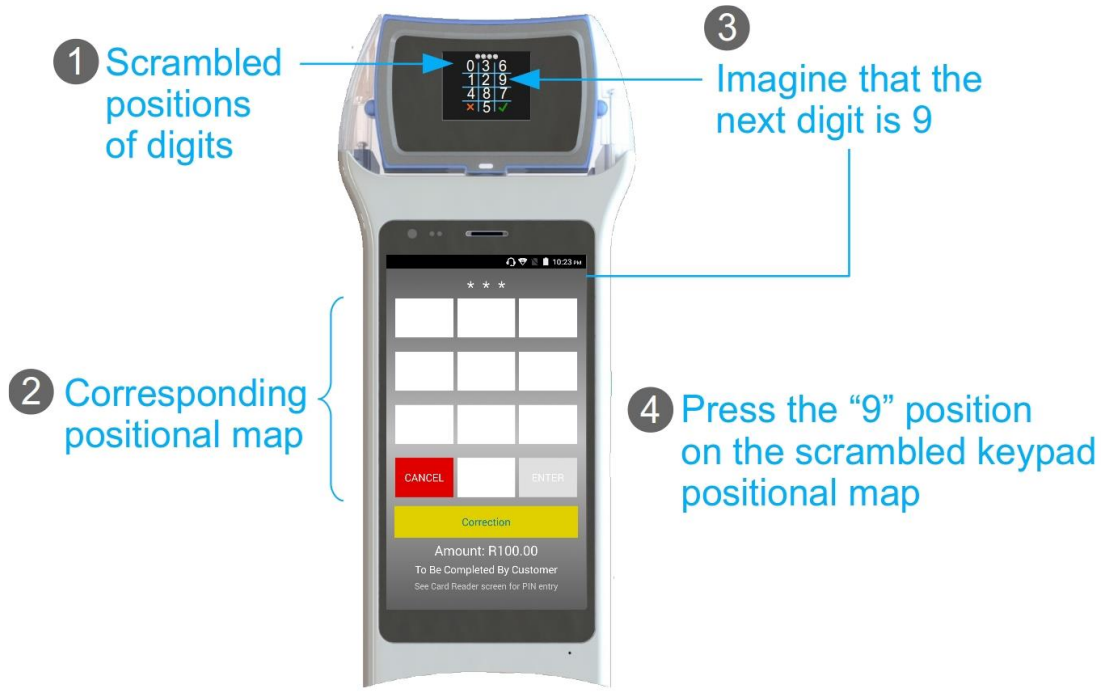

Figure 6 : Scrambled keypad PIN entry.

It is important to note that the actual PIN digits are never entered via the smartphone or Payment Blade software keypad. The keypad it only sends the representative coordinates for the keypad map that is displayed on the secure screen of the Payment Pebble® device. This is only possible because the cardholder, who knows the PIN, is able to visually locate the PIN digit on the Payment Pebble® device screen and locate its corresponding position on the grid on phone or Payment Blade application.

In the image below (Figure 6) it is shown how the cardholder will be instructed to enter the card's PIN via the text prompt "Enter PIN" that is shown at the top of the secure screen, with the keypad layout mask below the instruction. A ghost/disconnected keypad without numeric legends is provided on the smart phone or Payment Blade screen.

9.3. Device activation and deactivation

A Payment Pebble® device can be suspended or deactivated at the Transaction Service through the call centre or the merchant portal if implemented. Note that:

- A suspended Payment Pebble® cannot perform any transactions, but can be reactivated again once the issue has been cleared;
- If a Payment Pebble® is disabled, all keys in the device are cleared, and the must be returned to Thumbzup for destruction (alternatively proof of destruction should be supplied to Thumbzup)