“Un-fare Advantage”

Hacking the MBTA From 2008 to Present

Bobby Rauch

This presentation reflects research and analysis which I performed independently of my employer. This publication does not represent the views of my employer or past employers.

Whoami

Bobby Rauch - Twitter.com/@bobbyrsec

Offensive Security Engineer - Red Team - Fortune 500

Cyber Idiots Podcast

Bobbyrsec.com

MIT - Computer Science

Boston, Massachusetts - USA

Speaker at M0lecon Turin and Bsides London

OSCP OSWE

WHAT COULD POSSIBLY GO WRONG? —

Google pushes .zip and .mov domains onto the Internet, and the Internet pushes back

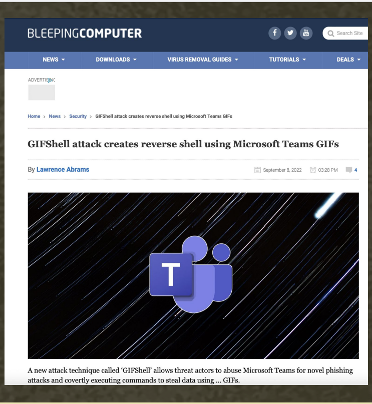
Will new TLDs undo decades of work to stop malicious links?

DAN GOODIN - 5/18/2023, 5:47 PM

Your CharlieCard can be hacked by an Android phone, MBTA admits

By Hiawatha Bray Globe Staff, Updated December 8, 2022, 1:28 p.m.

A CharlieCard being used at the State Street MBTA station in Boston. JOHN BLANDING/GLOBE STAFF


BLEEPINGCOMPUTER
Search Site
NEWS
DOWNLOADS
VIRUS REMOVAL GUIDES
TUTORIALS
DEALS
ADVERTISING
Home › News › Security › GIFShell attack creates reverse shell using Microsoft Teams GIFs
4

GIFShell attack creates reverse shell using Microsoft Teams GIFs

By Lawrence Abrams September 8, 2022 03:28 PM

A new attack technique called 'GIFShell' allows threat actors to abuse Microsoft Teams for novel phishing attacks and covertly executing commands to steal data using … GIFs.

Apple AirTag Bug Enables 'Good Samaritan' Attack

September 28, 2021 18 Comments

The new $30 AirTag tracking device from Apple has a feature that allows anyone who finds one of these tiny location beacons to scan it with a mobile phone and discover its owner's phone number if the AirTag has been set to lost mode. But according to new research, this same feature can be abused to redirect the Good Samaritan to an iCloud phishing page — or to any other malicious website.

Mailing List

Subscribe here

Search KrebsOnSecurity

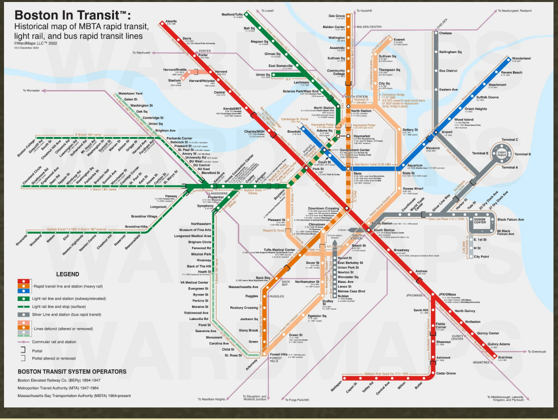
Recent Posts

- Apple AirTag Bug Enables 'Good Samaritan' Attack
- Indictment, Lawsuits Revive Trump-Alfa Bank Story
- Does Your Organization Have a Security.txt File?
- Trial Ends in Guilty Verdict for DDoS-for-Hire Boss
- Customer Care Giant TTEC Hit By Ransomware

Spam Nation

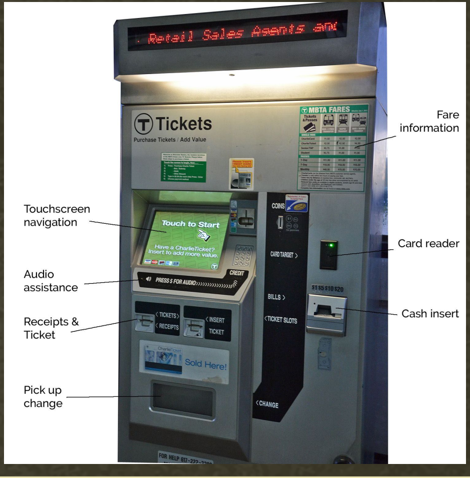
What We'll Cover

- Complex and legacy system design
- How vulnerability likelihood and severity can change with rapid changes in technology
- The importance of OSINT (Open-Source Intelligence) monitoring and threat intelligence
- The process of responsible vulnerability disclosure to a government agency without a Vulnerability Disclosure Program


Boston In Transit™:
Historical map of MBTA rapid transit, light rail, and bus rapid transit lines
©WardMaps LLC™ 2022
V2.0 December 2022
LEGEND
Rapid transit line and station (heavy rail)
Light rail line and station (subway/elevated)
Light rail line and stop (surface)
Silver Line and station (bus rapid transit)
Lines defunct (altered or removed)
Commuter rail and station
Portal
Portal altered or removed
BOSTON TRANSIT SYSTEM OPERATORS
Boston Elevated Railway Co. (BERy) 1894-1947
Metropolitan Transit Authority (MTA) 1947-1964
Massachusetts Bay Transportation Authority (MBTA) 1964-present

What's the MBTA/Charlie Card?

- Massachusetts Bay Transportation Authority (abbreviated MBTA and known colloquially as "the T")
- Fourth-busiest rapid transit system and the third-busiest light rail system in the United States.
- Electronic Fare Card is known as the CharlieCard, and can be refilled with credit/cash at fare machines around the city

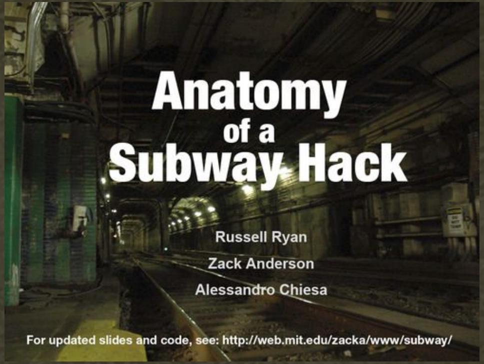


CharlieCard - 2008

- In 2008, a group of MIT students planned on appearing at Defcon and disclosing a set of vulnerabilities in the CharlieTicket (magstripe) and CharlieCard (Mifare Classic RFID card).

- The students were famously sued by the MBTA and were issued a gag order preventing them from disclosing the findings at Defcon

- The conference slides would later be posted online



Anatomy of a Subway Hack

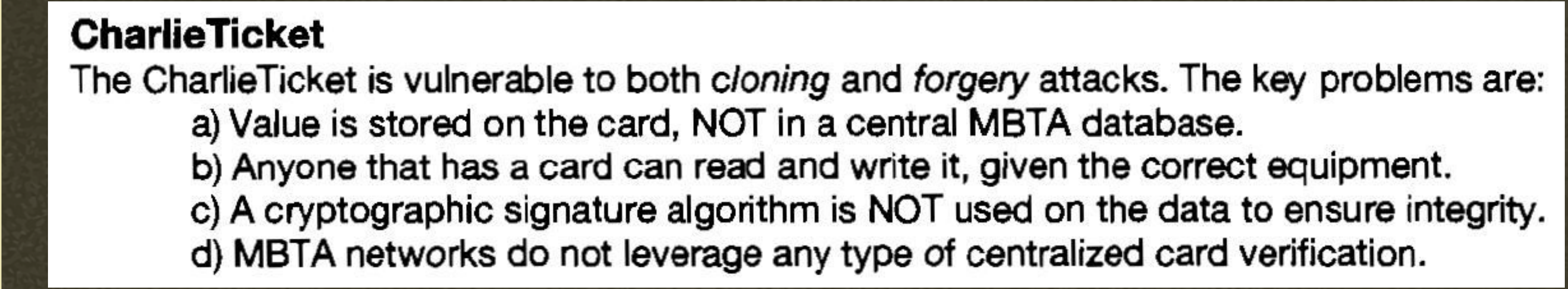
Russell Ryan

Zack Anderson

Alessandro Chiesa

For updated slides and code, see: http://web.mit.edu/zacka/www/subway/

CharlieCard - 2008 - Court Filing



CharlieTicket

The CharlieTicket is vulnerable to both *cloning* and *forgery* attacks. The key problems are:

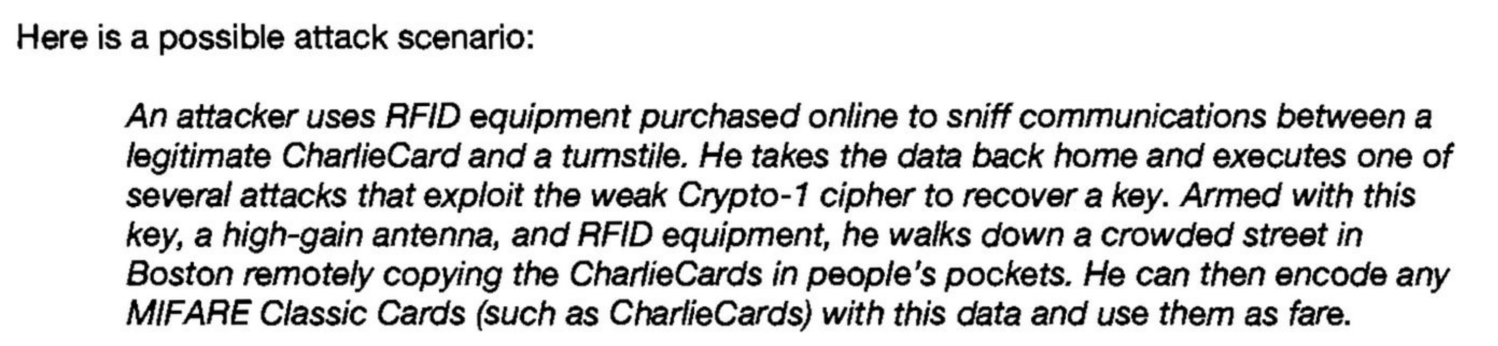
a) Value is stored on the card, NOT in a central MBTA database.

b) Anyone that has a card can read and write it, given the correct equipment.

c) A cryptographic signature algorithm is NOT used on the data to ensure integrity.

d) MBTA networks do not leverage any type of centralized card verification.

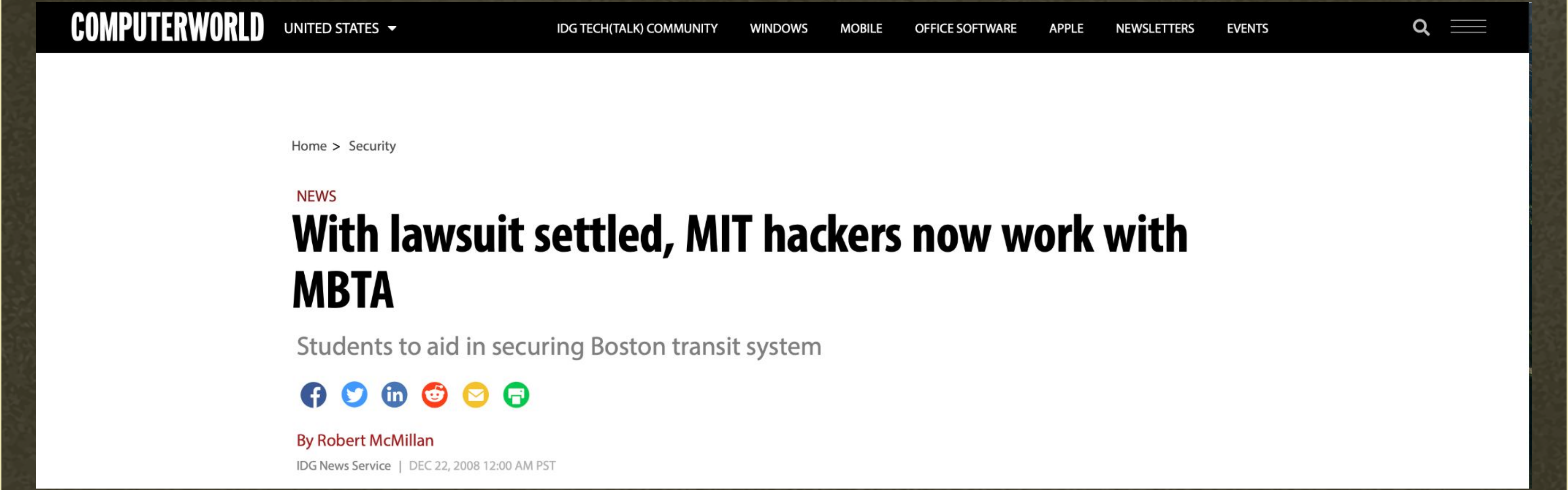
CharlieCard - 2008 - Court Filing



Here is a possible attack scenario:

> *An attacker uses RFID equipment purchased online to sniff communications between a legitimate CharlieCard and a turnstile. He takes the data back home and executes one of several attacks that exploit the weak Crypto-1 cipher to recover a key. Armed with this key, a high-gain antenna, and RFID equipment, he walks down a crowded street in Boston remotely copying the CharlieCards in people's pockets. He can then encode any MIFARE Classic Cards (such as CharlieCards) with this data and use them as fare.*

CharlieCard - 2008 - Fixed



NEWS

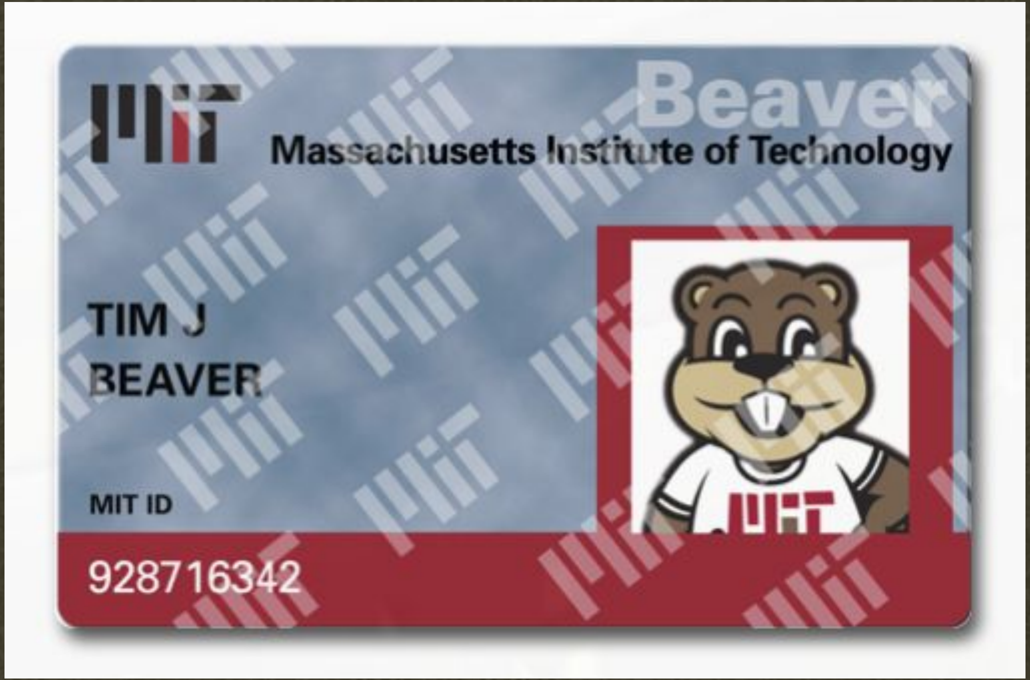
With lawsuit settled, MIT hackers now work with MBTA

Students to aid in securing Boston transit system

By Robert McMillan

IDG News Service | DEC 22, 2008 12:00 AM PST

CharlieCard - 2016

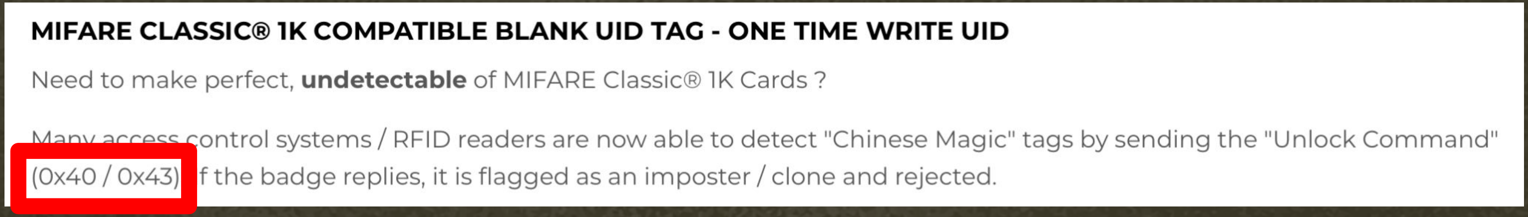


TIM J
BEAVER

MIT ID
928716342

CharlieCard - 2016

- The CharlieCard keeps track of the number of rides taken on the card itself.
- The monitoring script would watch for instances where a CharlieCard's transaction counter repeatedly decreased rather than increased
- The MBTA also implemented monitoring for cards that responded to "magic" commands, which are a distinct feature of a type of Mifare cards that are manufactured in China and are often used for low-cost card cloning.



MIFARE CLASSIC® 1K COMPATIBLE BLANK UID TAG - ONE TIME WRITE UID

Need to make perfect, **undetectable** of MIFARE Classic® 1K Cards ?

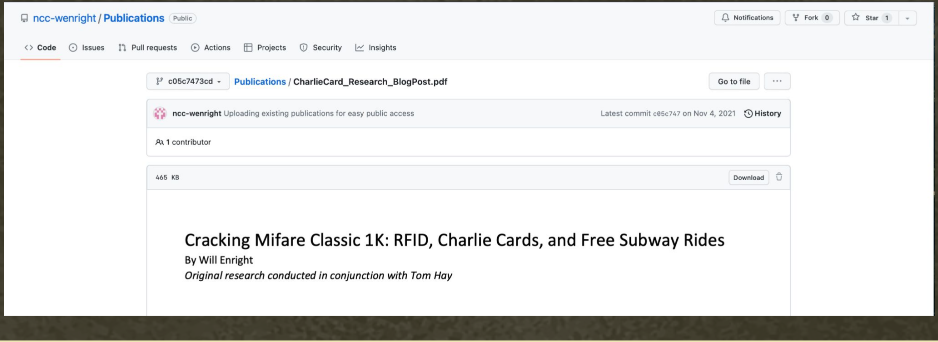
Many access control systems / RFID readers are now able to detect "Chinese Magic" tags by sending the "Unlock Command" (0x40 / 0x43) f the badge replies, it is flagged as an imposter / clone and rejected.

CharlieCard - 2019

- The research focuses on the vulnerabilities of Mifare Classic technology, and how a hardnested attack can be conducted with a Proxmark against the CharlieCard, by capturing a handshake between the card and the fare vending machine.

- He outlines that many of the key problems that MBTA had in their 2008 court filing still exist.

- He alludes to the fact that it may be possible to ride the Boston subway without paying by leveraging mobile NFC technology.



Publications / CharlieCard_Research_BlogPost.pdf

ncc-wenright Uploading existing publications for easy public access

Latest commit c05c747 on Nov 4, 2021

1 contributor

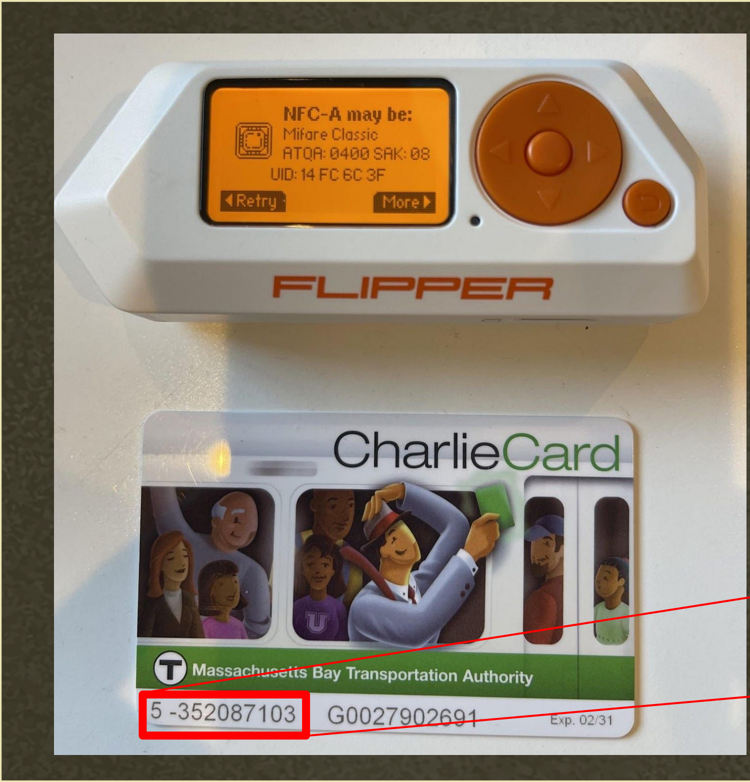
465 KB

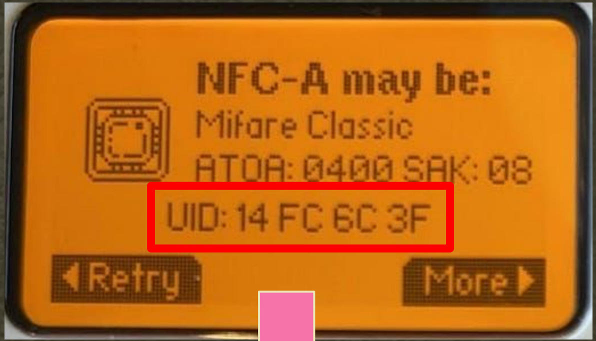
Cracking Mifare Classic 1K: RFID, Charlie Cards, and Free Subway Rides

By Will Enright

Original research conducted in conjunction with Tom Hay

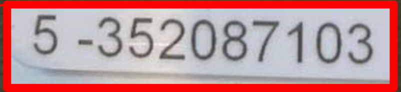
Flipper Zero - 2022





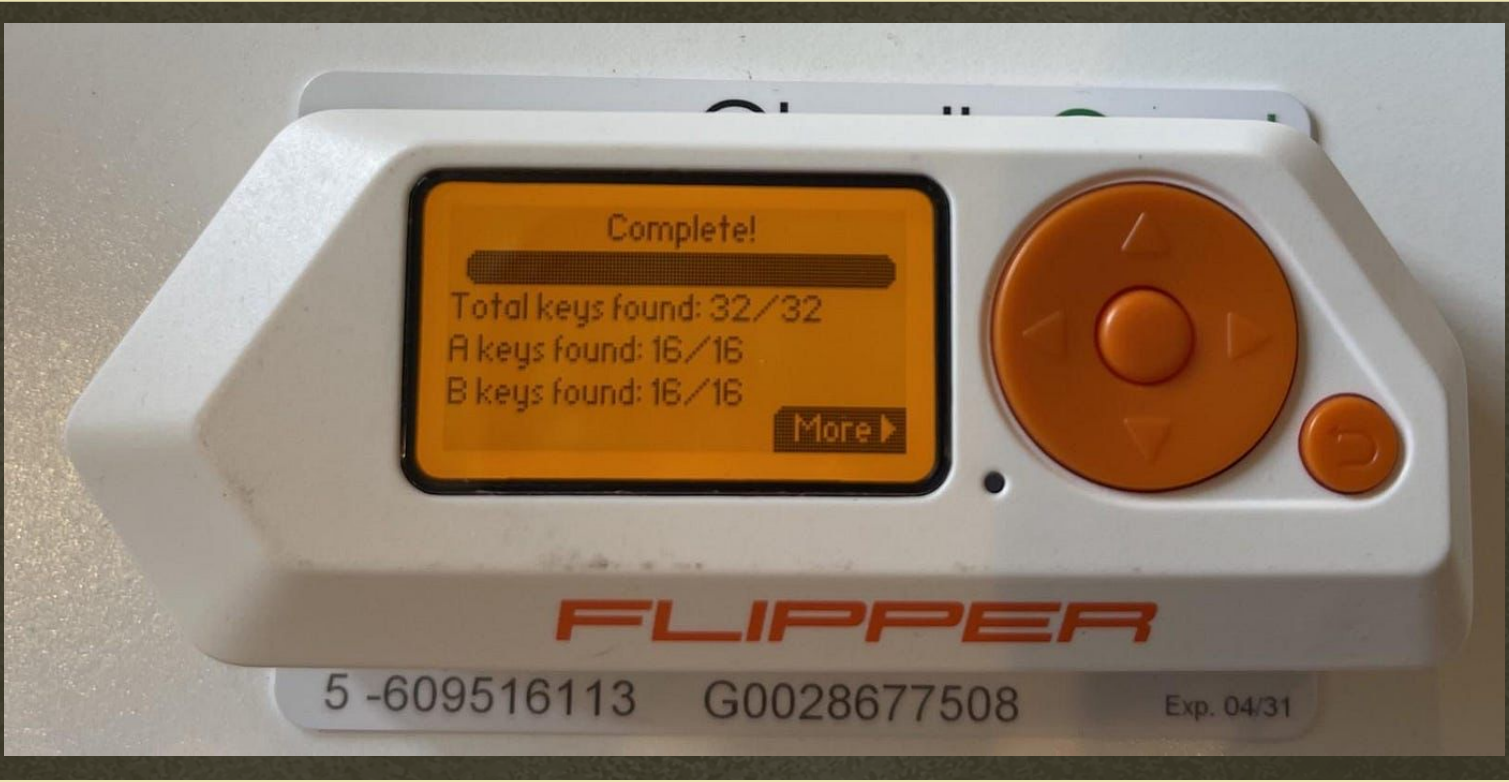
NFC-A may be:
Mifare Classic
ATQA: 0400 SAK: 08
UID: 14 FC 6C 3F

Hex



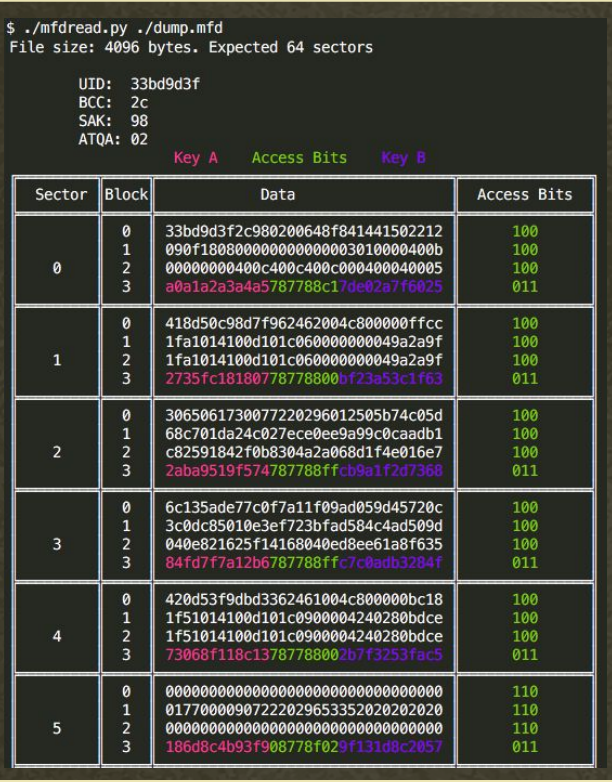
5 -352087103

Flipper Zero - Continued



```
Complete!
Total keys found: 32/32
A keys found: 16/16
B keys found: 16/16
More
```

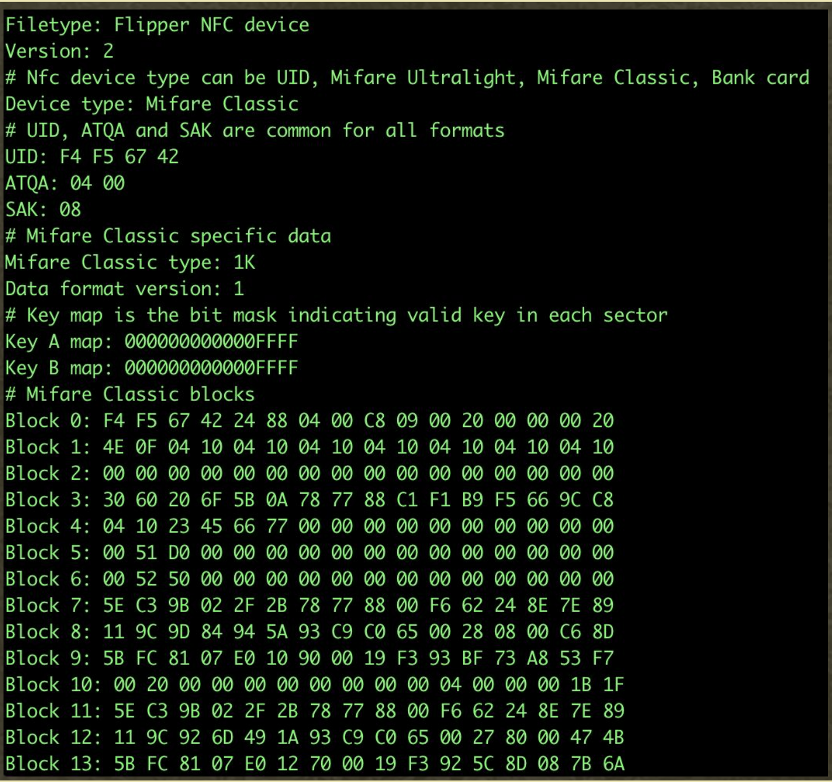
Mifare Classic Card Dump



```
$ ./mfdread.py ./dump.mfd
 File size: 4096 bytes. Expected 64 sectors

        UID:  33bd9d3f
        BCC:  2c
        SAK:  98
        ATQA: 02
                   Key A    Access Bits    Key B

  Sector   Block               Data                    Access Bits

              0    33bd9d3f2c980200648f841441502212        100
              1    090f1808000000000000003010000400b       100
    0         2    00000000400c400c400c000400040005        100
              3    a0a1a2a3a4a5787788c17de02a7f6025        011

              0    418d50c98d7f962462004c800000ffcc        100
              1    1fa1014100d101c060000000049a2a9f        100
    1         2    1fa1014100d101c060000000049a2a9f        100
              3    2735fc18180778778800bf23a53c1f63        011

              0    30650617300772202960125050b74c05d       100
              1    68c701da24c027ece0ee9a99c0caadb1        100
    2         2    c82591842f0b8304a2a068d1f4e016e7        100
              3    2aba9519f574787788ffcb9a1f2d7368        011

              0    6c135ade77c0f7a11f09ad059d45720c        100
              1    3c0dc85010e3ef723bfad584c4ad509d        100
    3         2    040e821625f14168040ed8ee61a8f635        100
              3    84fd7f7a12b6787788ffc7c0adb3284f        011

              0    420d53f9dbd3362461004c800000bc18        100
              1    1f51014100d101c0900004240280bdce        100
    4         2    1f51014100d101c0900004240280bdce        100
              3    73068f118c13787788002b7f3253fac5        011

              0    00000000000000000000000000000000        110
              1    01770000907222029653352020202020        110
    5         2    00000000000000000000000000000000        110
              3    186d8c4b93f908778f029f131d8c2057        011
```

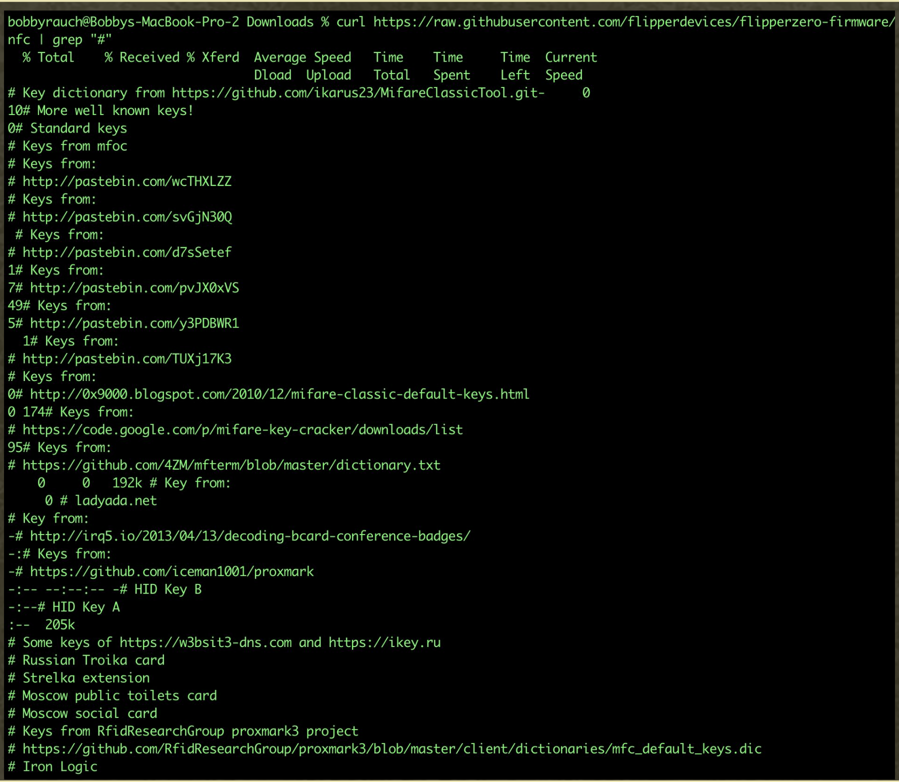
16 sectors x 2 keys = 32 Total Keys

Flipper Zero - Card Dump



```
Filetype: Flipper NFC device
Version: 2
# Nfc device type can be UID, Mifare Ultralight, Mifare Classic, Bank card
Device type: Mifare Classic
# UID, ATQA and SAK are common for all formats
UID: F4 F5 67 42
ATQA: 04 00
SAK: 08
# Mifare Classic specific data
Mifare Classic type: 1K
Data format version: 1
# Key map is the bit mask indicating valid key in each sector
Key A map: 000000000000FFFF
Key B map: 000000000000FFFF
# Mifare Classic blocks
Block 0: F4 F5 67 42 24 88 04 00 C8 09 00 20 00 00 00 20
Block 1: 4E 0F 04 10 04 10 04 10 04 10 04 10 04 10 04 10
Block 2: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Block 3: 30 60 20 6F 5B 0A 78 77 88 C1 F1 B9 F5 66 9C C8
Block 4: 04 10 23 45 66 77 00 00 00 00 00 00 00 00 00 00
Block 5: 00 51 D0 00 00 00 00 00 00 00 00 00 00 00 00 00
Block 6: 00 52 50 00 00 00 00 00 00 00 00 00 00 00 00 00
Block 7: 5E C3 9B 02 2F 2B 78 77 88 00 F6 62 24 8E 7E 89
Block 8: 11 9C 9D 84 94 5A 93 C9 C0 65 00 28 08 00 C6 8D
Block 9: 5B FC 81 07 E0 10 90 00 19 F3 93 BF 73 A8 53 F7
Block 10: 00 20 00 00 00 00 00 00 00 00 04 00 00 00 1B 1F
Block 11: 5E C3 9B 02 2F 2B 78 77 88 00 F6 62 24 8E 7E 89
Block 12: 11 9C 92 6D 49 1A 93 C9 C0 65 00 27 80 00 47 4B
Block 13: 5B FC 81 07 E0 12 70 00 19 F3 92 5C 8D 08 7B 6A
```

Flipper Zero Firmware



```
bobbyrauch@Bobbys-MacBook-Pro-2 Downloads % curl https://raw.githubusercontent.com/flipperdevices/flipperzero-firmware/
nfc | grep "#"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
# Key dictionary from https://github.com/ikarus23/MifareClassicTool.git-     0
10# More well known keys!
0# Standard keys
# Keys from mfoc
# Keys from:
# http://pastebin.com/wcTHXLZZ
# Keys from:
# http://pastebin.com/svGjN30Q
 # Keys from:
# http://pastebin.com/d7sSetef
1# Keys from:
7# http://pastebin.com/pvJX0xVS
49# Keys from:
5# http://pastebin.com/y3PDBWR1
  1# Keys from:
# http://pastebin.com/TUXj17K3
# Keys from:
0# http://0x9000.blogspot.com/2010/12/mifare-classic-default-keys.html
0 174# Keys from:
# https://code.google.com/p/mifare-key-cracker/downloads/list
95# Keys from:
# https://github.com/4ZM/mfterm/blob/master/dictionary.txt
    0     0   192k # Key from:
     0 # ladyada.net
# Key from:
-# http://irq5.io/2013/04/13/decoding-bcard-conference-badges/
-:# Keys from:
-# https://github.com/iceman1001/proxmark
-:-- --:--:-- -# HID Key B
-:--# HID Key A
:--  205k
# Some keys of https://w3bsit3-dns.com and https://ikey.ru
# Russian Troika card
# Strelka extension
# Moscow public toilets card
# Moscow social card
# Keys from RfidResearchGroup proxmark3 project
# https://github.com/RfidResearchGroup/proxmark3/blob/master/client/dictionaries/mfc_default_keys.dic
# Iron Logic
```

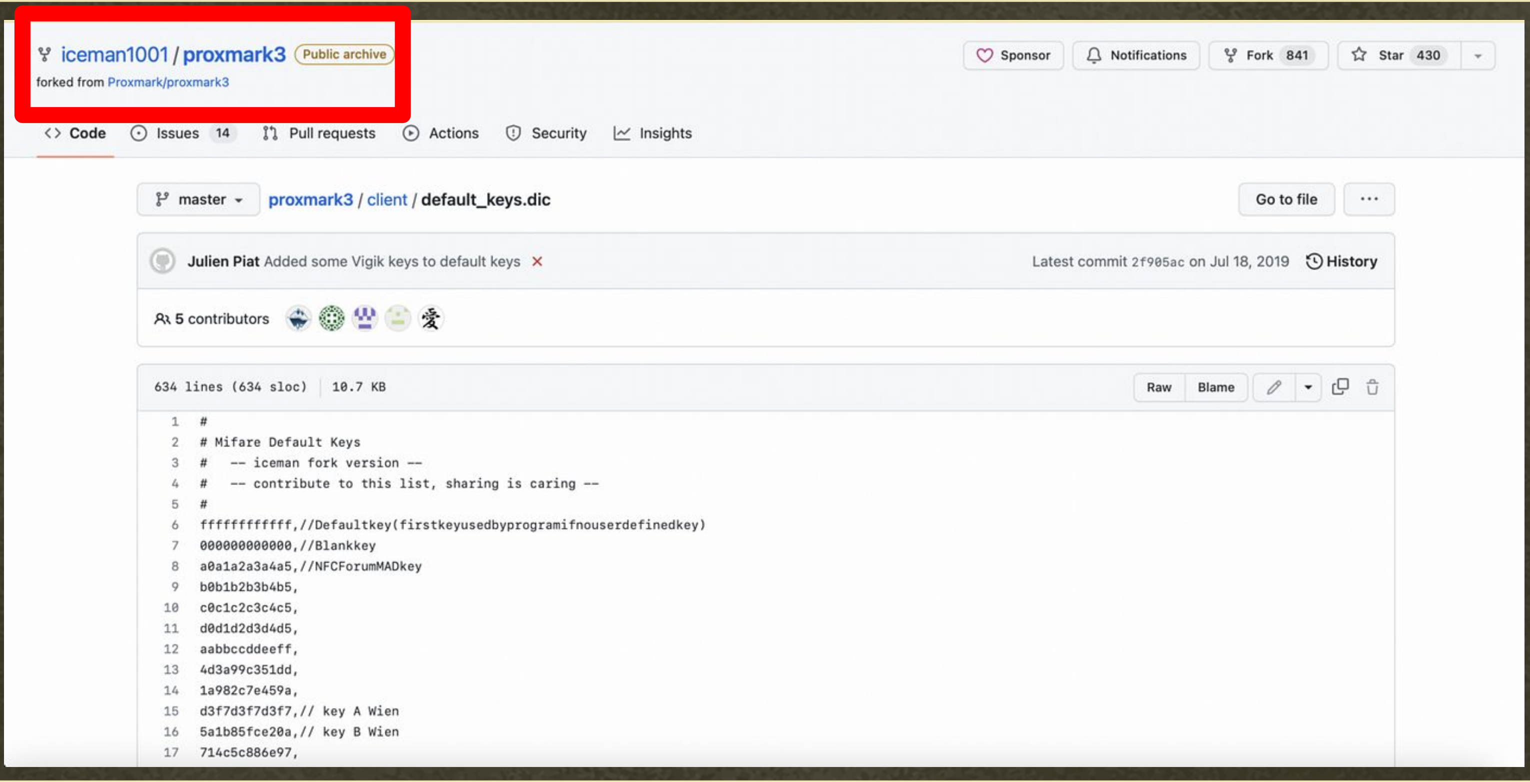
Working Backwards

```
# Mifare Classic blocks
Block 0: F4 F5 67 42 24 88 04 00 C8 09 00 20 00 00 00 20
Block 1: 4E 0F 04 10 04 10 04 10 04 10 04 10 04 10 04 10
Block 2: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Block 3: 30 60 20 6F 5B 0A 78 77 88 C1 F1 B9 F5 66 9C C8
```

Working Backwards

```
# Keys from:
# https://github.com/iceman1001/proxmark
…
# HID Key B
204752454154
21A600056CB0
22729A9BD40F
…
3060206F5B0A
```

Working Backwards



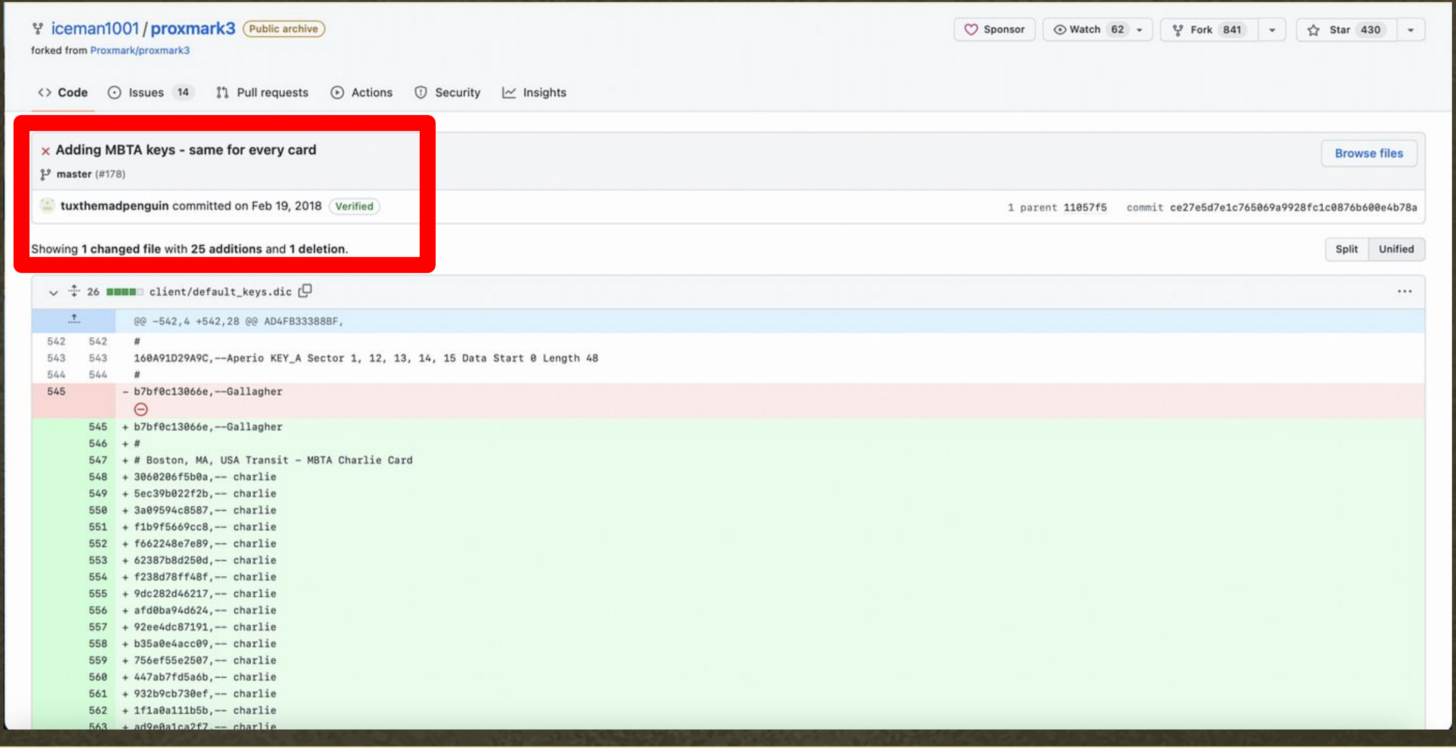
Julien Piat Added some Vigik keys to default keys ✕

Latest commit 2f905ac on Jul 18, 2019

634 lines (634 sloc) | 10.7 KB

```
#
# Mifare Default Keys
#   -- iceman fork version --
#   -- contribute to this list, sharing is caring --
#
ffffffffffff,//Defaultkey(firstkeyusedbyprogramifnouserdefinedkey)
000000000000,//Blankkey
a0a1a2a3a4a5,//NFCForumMADkey
b0b1b2b3b4b5,
c0c1c2c3c4c5,
d0d1d2d3d4d5,
aabbccddeeff,
4d3a99c351dd,
1a982c7e459a,
d3f7d3f7d3f7,// key A Wien
5a1b85fce20a,// key B Wien
714c5c886e97,
```

Working Backwards



✕ Adding MBTA keys - same for every card

master (#178)

tuxthemadpenguin committed on Feb 19, 2018 Verified

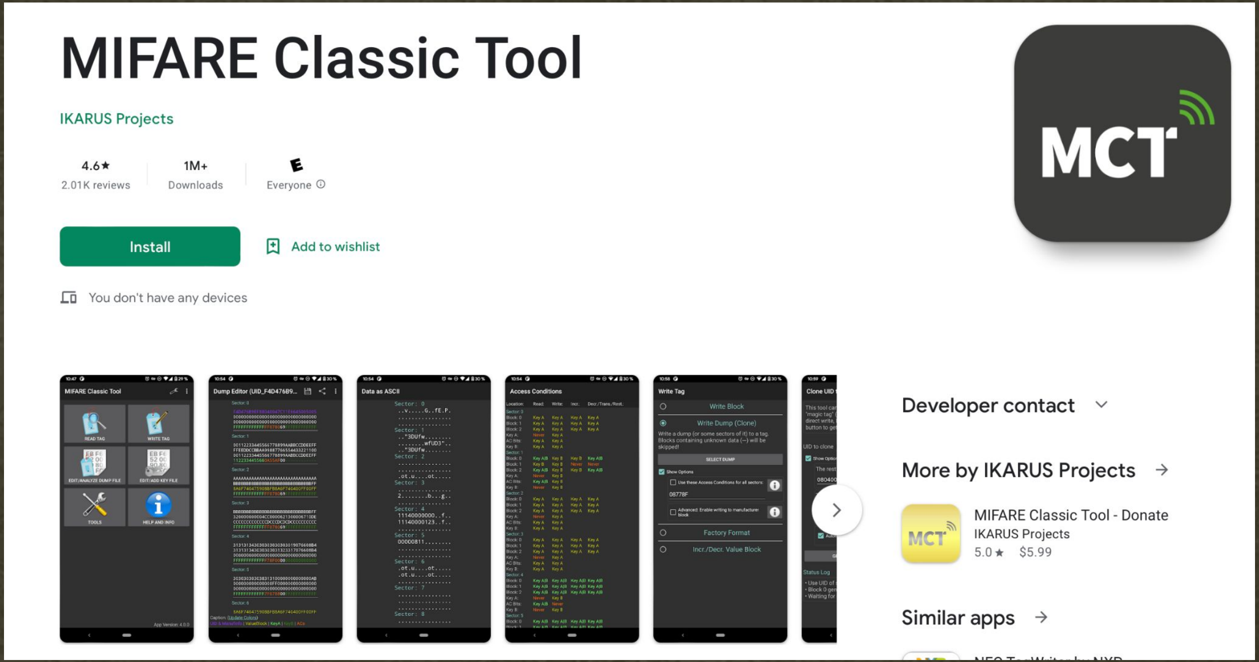
1 parent 11057f5 commit ce27e5d7e1c765069a9928fc1c0876b600e4b78a

Showing **1 changed file** with **25 additions** and **1 deletion**.

26 client/default_keys.dic

```
@@ -542,4 +542,28 @@ AD4FB33388BF,
  #
  160A91D29A9C,--Aperio KEY_A Sector 1, 12, 13, 14, 15 Data Start 0 Length 48
  #
- b7bf0c13066e,--Gallagher
+ b7bf0c13066e,--Gallagher
+ #
+ # Boston, MA, USA Transit - MBTA Charlie Card
+ 3060206f5b0a,-- charlie
+ 5ec39b022f2b,-- charlie
+ 3a09594c8587,-- charlie
+ f1b9f5669cc8,-- charlie
+ f662248e7e89,-- charlie
+ 62387b8d250d,-- charlie
+ f238d78ff48f,-- charlie
+ 9dc282d46217,-- charlie
+ afd0ba94d624,-- charlie
+ 92ee4dc87191,-- charlie
+ b35a0e4acc09,-- charlie
+ 756ef55e2507,-- charlie
+ 447ab7fd5a6b,-- charlie
+ 932b9cb730ef,-- charlie
+ 1f1a0a111b5b,-- charlie
+ ad9e0a1ca2f7,-- charlie
```

Mifare Classic Toolkit



MIFARE Classic Tool

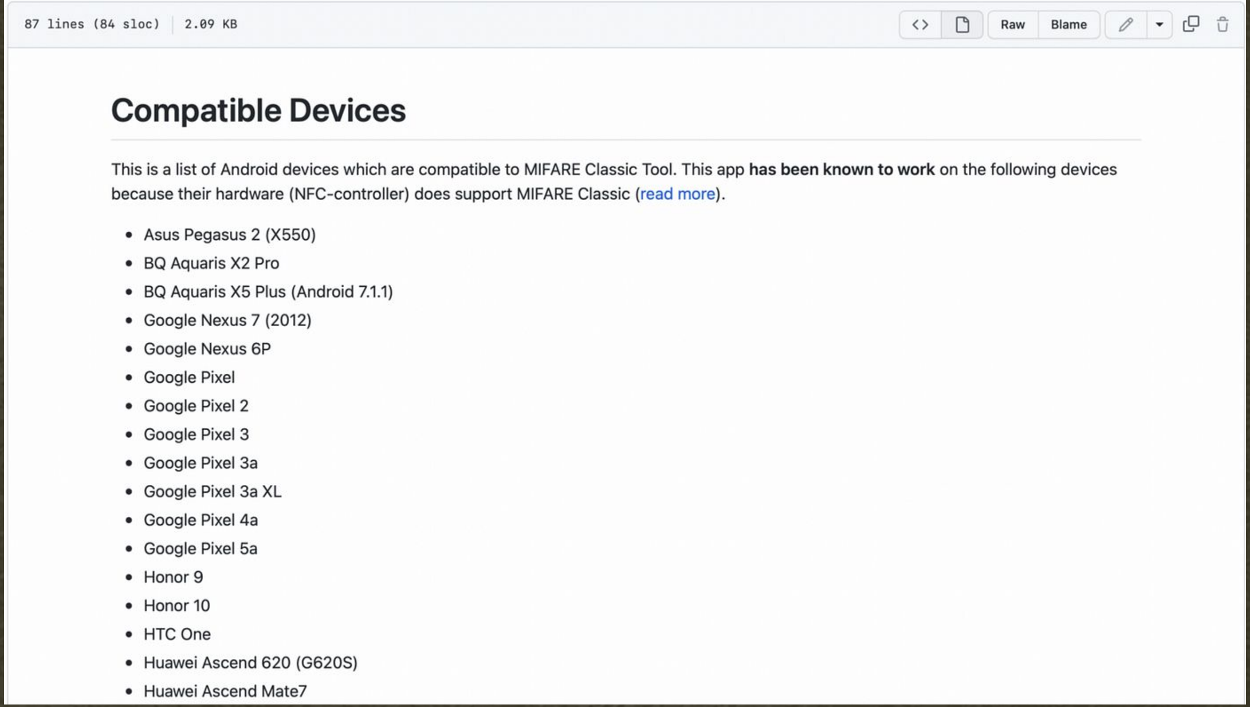
IKARUS Projects

4.6★ 2.01K reviews | 1M+ Downloads | E Everyone ⓘ

Install | Add to wishlist

You don't have any devices

Mifare Classic Toolkit

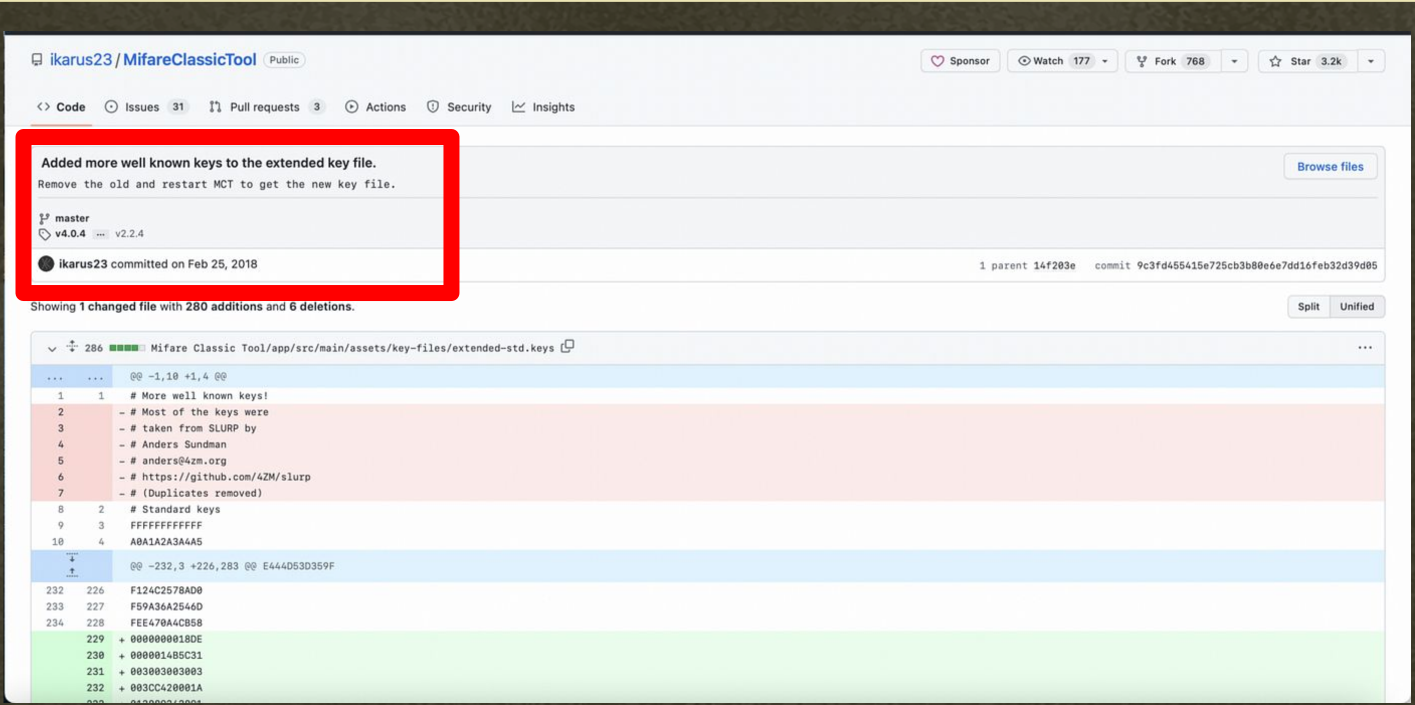


Compatible Devices

This is a list of Android devices which are compatible to MIFARE Classic Tool. This app **has been known to work** on the following devices because their hardware (NFC-controller) does support MIFARE Classic (read more).

- Asus Pegasus 2 (X550)
- BQ Aquaris X2 Pro
- BQ Aquaris X5 Plus (Android 7.1.1)
- Google Nexus 7 (2012)
- Google Nexus 6P
- Google Pixel
- Google Pixel 2
- Google Pixel 3
- Google Pixel 3a
- Google Pixel 3a XL
- Google Pixel 4a
- Google Pixel 5a
- Honor 9
- Honor 10
- HTC One
- Huawei Ascend 620 (G620S)
- Huawei Ascend Mate7

Mifare Classic Toolkit



Added more well known keys to the extended key file.

Remove the old and restart MCT to get the new key file.

master
v4.0.4 ... v2.2.4

ikarus23 committed on Feb 25, 2018

1 parent 14f203e commit 9c3fd455415e725cb3b80e6e7dd16feb32d39d05

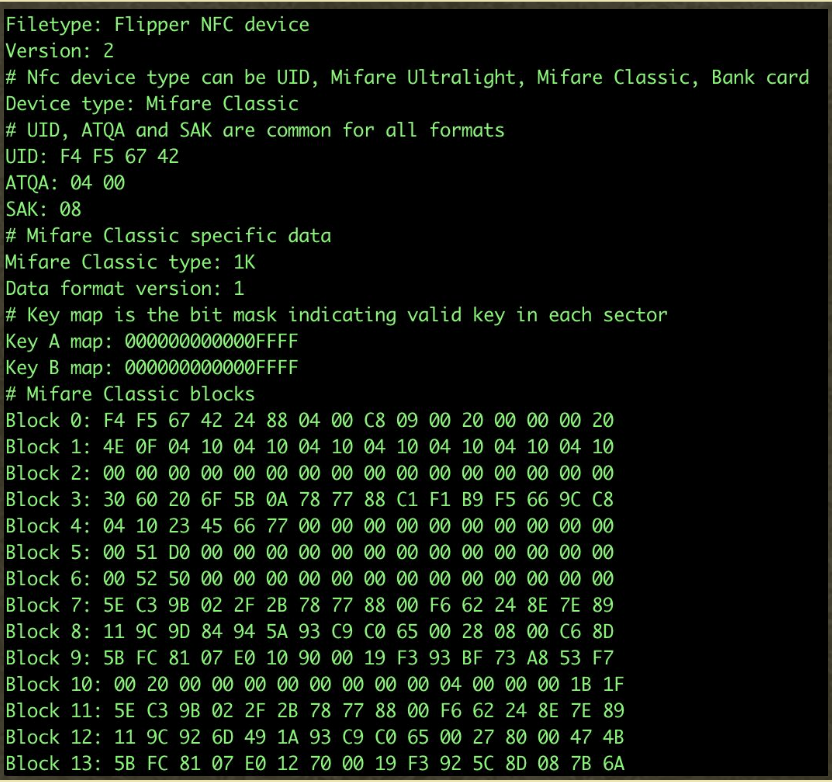
Showing **1 changed file** with **280 additions** and **6 deletions**.

286 Mifare Classic Tool/app/src/main/assets/key-files/extended-std.keys

```
@@ -1,10 +1,4 @@
  # More well known keys!
- # Most of the keys were
- # taken from SLURP by
- # Anders Sundman
- # anders@4zm.org
- # https://github.com/4ZM/slurp
- # (Duplicates removed)
  # Standard keys
  FFFFFFFFFFFF
  A0A1A2A3A4A5
@@ -232,3 +226,283 @@ E444D53D359F
  F124C2578AD0
  F59A36A2546D
  FEE470A4CB58
+ 0000000018DE
+ 0000014B5C31
+ 003003003003
+ 003CC420001A
```

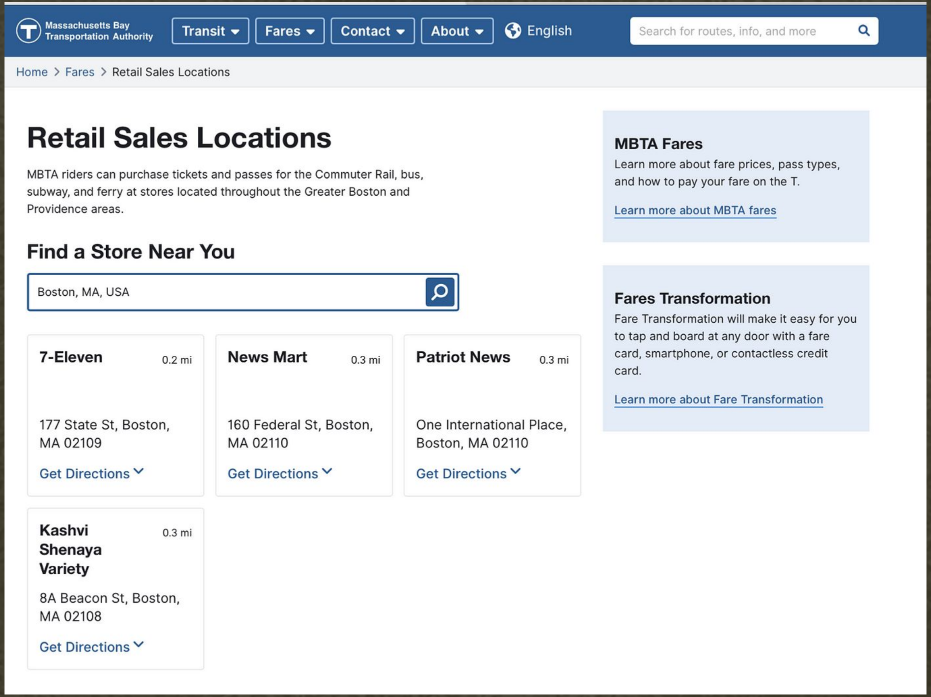
Definitive Proof of Stored Value

Where's the Value?



```
Filetype: Flipper NFC device
Version: 2
# Nfc device type can be UID, Mifare Ultralight, Mifare Classic, Bank card
Device type: Mifare Classic
# UID, ATQA and SAK are common for all formats
UID: F4 F5 67 42
ATQA: 04 00
SAK: 08
# Mifare Classic specific data
Mifare Classic type: 1K
Data format version: 1
# Key map is the bit mask indicating valid key in each sector
Key A map: 000000000000FFFF
Key B map: 000000000000FFFF
# Mifare Classic blocks
Block 0: F4 F5 67 42 24 88 04 00 C8 09 00 20 00 00 00 20
Block 1: 4E 0F 04 10 04 10 04 10 04 10 04 10 04 10 04 10
Block 2: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Block 3: 30 60 20 6F 5B 0A 78 77 88 C1 F1 B9 F5 66 9C C8
Block 4: 04 10 23 45 66 77 00 00 00 00 00 00 00 00 00 00
Block 5: 00 51 D0 00 00 00 00 00 00 00 00 00 00 00 00 00
Block 6: 00 52 50 00 00 00 00 00 00 00 00 00 00 00 00 00
Block 7: 5E C3 9B 02 2F 2B 78 77 88 00 F6 62 24 8E 7E 89
Block 8: 11 9C 9D 84 94 5A 93 C9 C0 65 00 28 08 00 C6 8D
Block 9: 5B FC 81 07 E0 10 90 00 19 F3 93 BF 73 A8 53 F7
Block 10: 00 20 00 00 00 00 00 00 00 00 04 00 00 00 1B 1F
Block 11: 5E C3 9B 02 2F 2B 78 77 88 00 F6 62 24 8E 7E 89
Block 12: 11 9C 92 6D 49 1A 93 C9 C0 65 00 27 80 00 47 4B
Block 13: 5B FC 81 07 E0 12 70 00 19 F3 92 5C 8D 08 7B 6A
```

MBTA - Retail Sales Locations



Massachusetts Bay Transportation Authority
Transit
Fares
Contact
About
English
Search for routes, info, and more

Home > Fares > Retail Sales Locations

Retail Sales Locations

MBTA riders can purchase tickets and passes for the Commuter Rail, bus, subway, and ferry at stores located throughout the Greater Boston and Providence areas.

Find a Store Near You

Boston, MA, USA

7-Eleven 0.2 mi

177 State St, Boston, MA 02109

Get Directions

News Mart 0.3 mi

160 Federal St, Boston, MA 02110

Get Directions

Patriot News 0.3 mi

One International Place, Boston, MA 02110

Get Directions

Kashvi Shenaya Variety 0.3 mi

8A Beacon St, Boston, MA 02108

Get Directions

MBTA Fares

Learn more about fare prices, pass types, and how to pay your fare on the T.

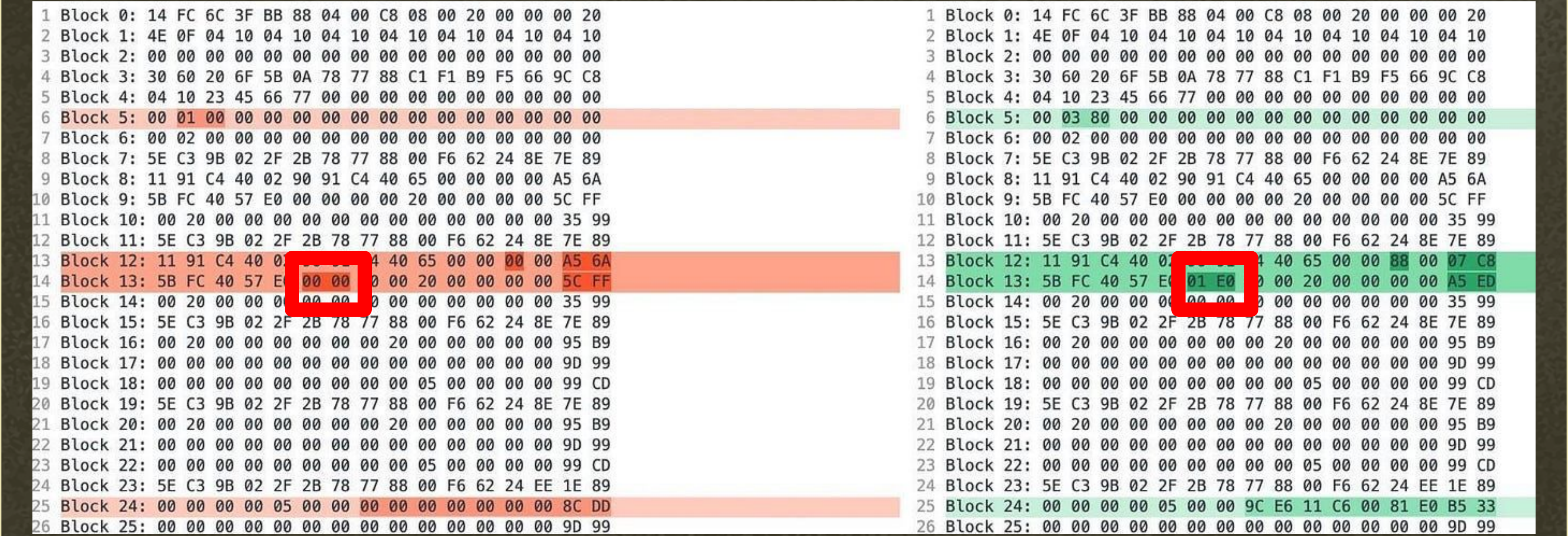
Learn more about MBTA fares

Fares Transformation

Fare Transformation will make it easy for you to tap and board at any door with a fare card, smartphone, or contactless credit card.

Learn more about Fare Transformation

MBTA - Retail Sales Locations



```
Block 0: 14 FC 6C 3F BB 88 04 00 C8 08 00 20 00 00 00 20
Block 1: 4E 0F 04 10 04 10 04 10 04 10 04 10 04 10 04 10
Block 2: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Block 3: 30 60 20 6F 5B 0A 78 77 88 C1 F1 B9 F5 66 9C C8
Block 4: 04 10 23 45 66 77 00 00 00 00 00 00 00 00 00 00
Block 5: 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Block 6: 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Block 7: 5E C3 9B 02 2F 2B 78 77 88 00 F6 62 24 8E 7E 89
Block 8: 11 91 C4 40 02 90 91 C4 40 65 00 00 00 00 A5 6A
Block 9: 5B FC 40 57 E0 00 00 00 00 20 00 00 00 00 5C FF
Block 10: 00 20 00 00 00 00 00 00 00 00 00 00 00 00 35 99
Block 11: 5E C3 9B 02 2F 2B 78 77 88 00 F6 62 24 8E 7E 89
Block 12: 11 91 C4 40 02 90 91 C4 40 65 00 00 00 00 A5 6A
Block 13: 5B FC 40 57 E0 00 00 00 00 20 00 00 00 00 5C FF
Block 14: 00 20 00 00 00 00 00 00 00 00 00 00 00 00 35 99
Block 15: 5E C3 9B 02 2F 2B 78 77 88 00 F6 62 24 8E 7E 89
Block 16: 00 20 00 00 00 00 00 00 20 00 00 00 00 00 95 B9
Block 17: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9D 99
Block 18: 00 00 00 00 00 00 00 00 00 05 00 00 00 00 99 CD
Block 19: 5E C3 9B 02 2F 2B 78 77 88 00 F6 62 24 8E 7E 89
Block 20: 00 20 00 00 00 00 00 00 20 00 00 00 00 00 95 B9
Block 21: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9D 99
Block 22: 00 00 00 00 00 00 00 00 00 05 00 00 00 00 99 CD
Block 23: 5E C3 9B 02 2F 2B 78 77 88 00 F6 62 24 EE 1E 89
Block 24: 00 00 00 00 05 00 00 00 00 00 00 00 00 00 8C DD
Block 25: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9D 99
```

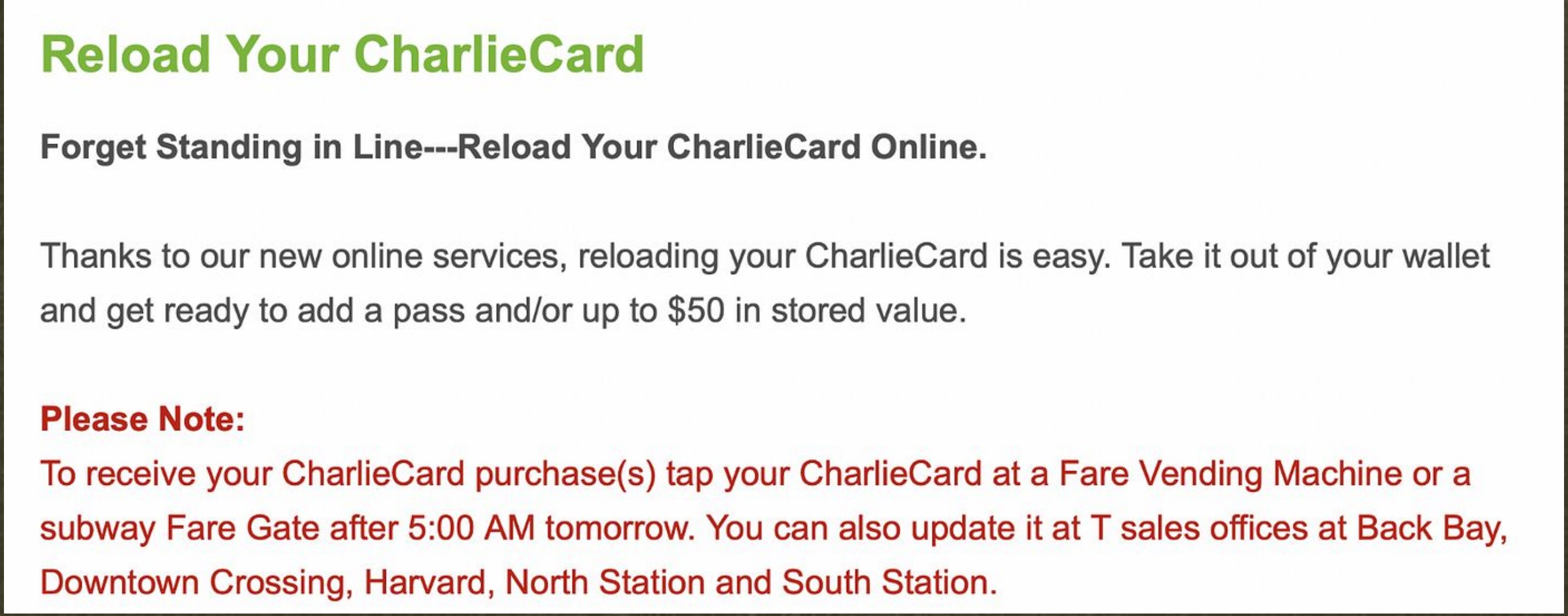
```
Block 0: 14 FC 6C 3F BB 88 04 00 C8 08 00 20 00 00 00 20
Block 1: 4E 0F 04 10 04 10 04 10 04 10 04 10 04 10 04 10
Block 2: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Block 3: 30 60 20 6F 5B 0A 78 77 88 C1 F1 B9 F5 66 9C C8
Block 4: 04 10 23 45 66 77 00 00 00 00 00 00 00 00 00 00
Block 5: 00 03 80 00 00 00 00 00 00 00 00 00 00 00 00 00
Block 6: 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Block 7: 5E C3 9B 02 2F 2B 78 77 88 00 F6 62 24 8E 7E 89
Block 8: 11 91 C4 40 02 90 91 C4 40 65 00 00 00 00 A5 6A
Block 9: 5B FC 40 57 E0 00 00 00 00 20 00 00 00 00 5C FF
Block 10: 00 20 00 00 00 00 00 00 00 00 00 00 00 00 35 99
Block 11: 5E C3 9B 02 2F 2B 78 77 88 00 F6 62 24 8E 7E 89
Block 12: 11 91 C4 40 02 90 91 C4 40 65 00 00 88 00 07 C8
Block 13: 5B FC 40 57 E0 01 E0 00 00 20 00 00 00 00 A5 ED
Block 14: 00 20 00 00 00 00 00 00 00 00 00 00 00 00 35 99
Block 15: 5E C3 9B 02 2F 2B 78 77 88 00 F6 62 24 8E 7E 89
Block 16: 00 20 00 00 00 00 00 00 20 00 00 00 00 00 95 B9
Block 17: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9D 99
Block 18: 00 00 00 00 00 00 00 00 00 05 00 00 00 00 99 CD
Block 19: 5E C3 9B 02 2F 2B 78 77 88 00 F6 62 24 8E 7E 89
Block 20: 00 20 00 00 00 00 00 00 20 00 00 00 00 00 95 B9
Block 21: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9D 99
Block 22: 00 00 00 00 00 00 00 00 00 05 00 00 00 00 99 CD
Block 23: 5E C3 9B 02 2F 2B 78 77 88 00 F6 62 24 EE 1E 89
Block 24: 00 00 00 00 05 00 00 9C E6 11 C6 00 81 E0 B5 33
Block 25: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9D 99
```

01 E0 ≈ 0x01E0 = 480 -> 480 ÷ 200 = $2.40

Obfuscation

Need for Stored Value

Proof of Server-Side Validation



Reload Your CharlieCard

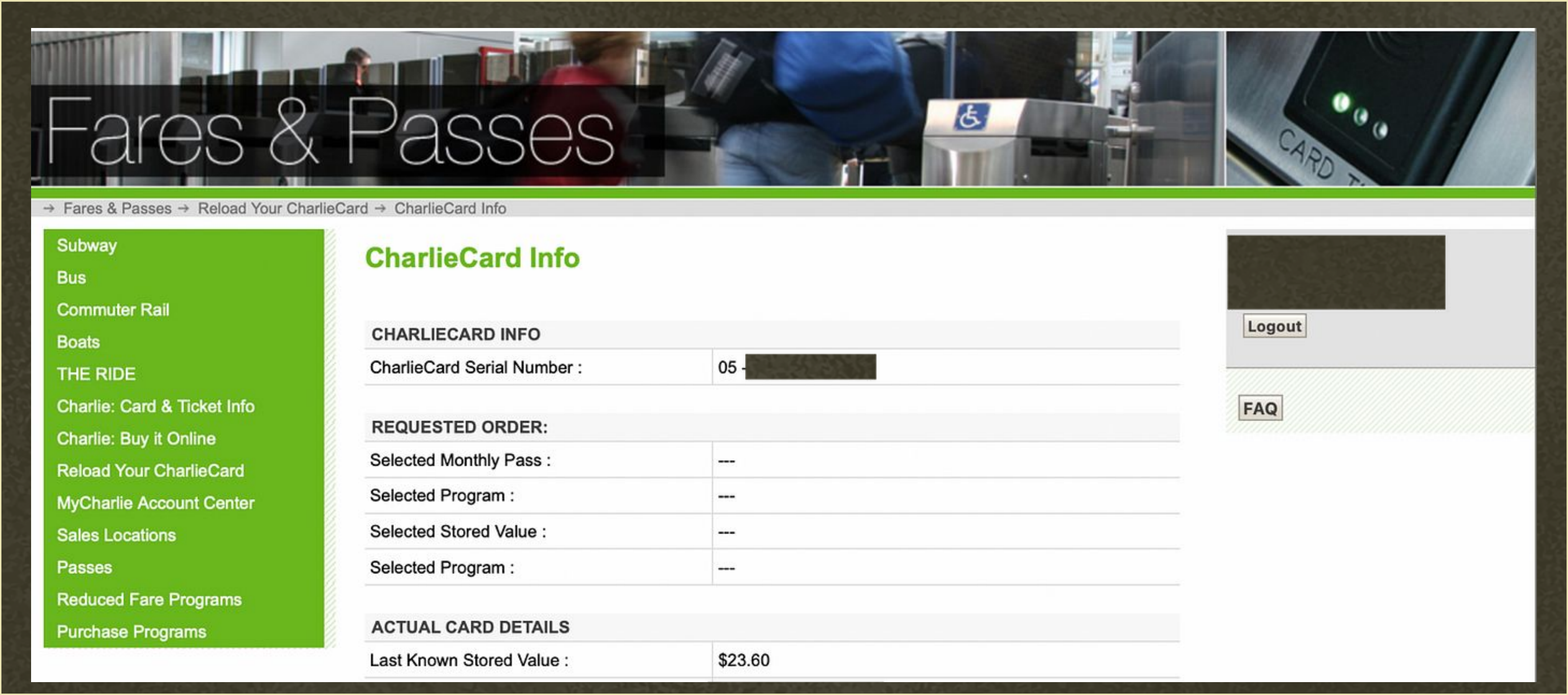
Forget Standing in Line---Reload Your CharlieCard Online.

Thanks to our new online services, reloading your CharlieCard is easy. Take it out of your wallet and get ready to add a pass and/or up to $50 in stored value.

Please Note:

To receive your CharlieCard purchase(s) tap your CharlieCard at a Fare Vending Machine or a subway Fare Gate after 5:00 AM tomorrow. You can also update it at T sales offices at Back Bay, Downtown Crossing, Harvard, North Station and South Station.

Online Reloads



[redacted]

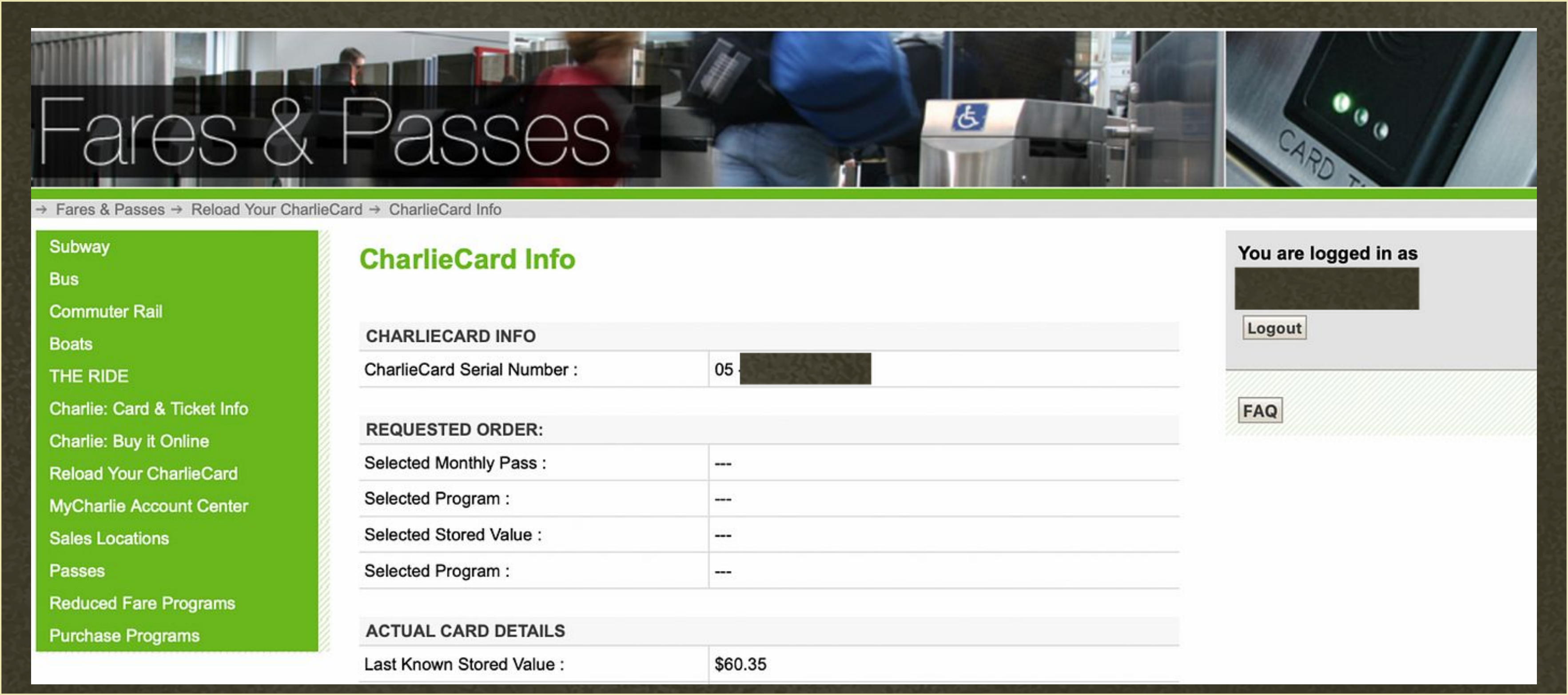
CharlieCard Info

CHARLIECARD INFO	
CharlieCard Serial Number :	05 -[redacted]

REQUESTED ORDER:	
Selected Monthly Pass :	---
Selected Program :	---
Selected Stored Value :	---
Selected Program :	---

ACTUAL CARD DETAILS	
Last Known Stored Value :	$23.60

Online Reloads



Fares & Passes

→ Fares & Passes → Reload Your CharlieCard → CharlieCard Info

- Subway
- Bus
- Commuter Rail
- Boats
- THE RIDE
- Charlie: Card & Ticket Info
- Charlie: Buy it Online
- Reload Your CharlieCard
- MyCharlie Account Center
- Sales Locations
- Passes
- Reduced Fare Programs
- Purchase Programs

CharlieCard Info

CHARLIECARD INFO	
CharlieCard Serial Number :	05 [redacted]

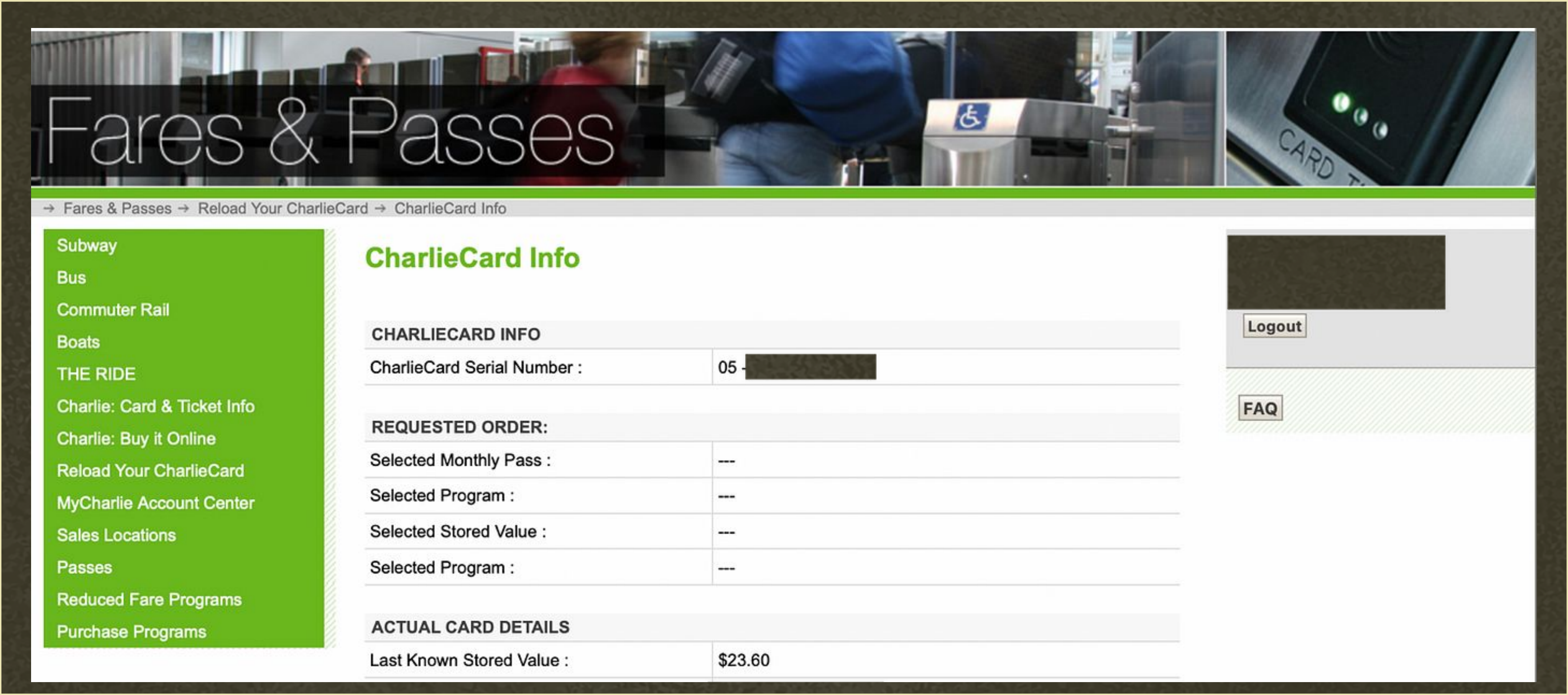
REQUESTED ORDER:	
Selected Monthly Pass :	---
Selected Program :	---
Selected Stored Value :	---
Selected Program :	---

ACTUAL CARD DETAILS	
Last Known Stored Value :	$60.35

You are logged in as

[redacted]

Online Reloads



[redacted]

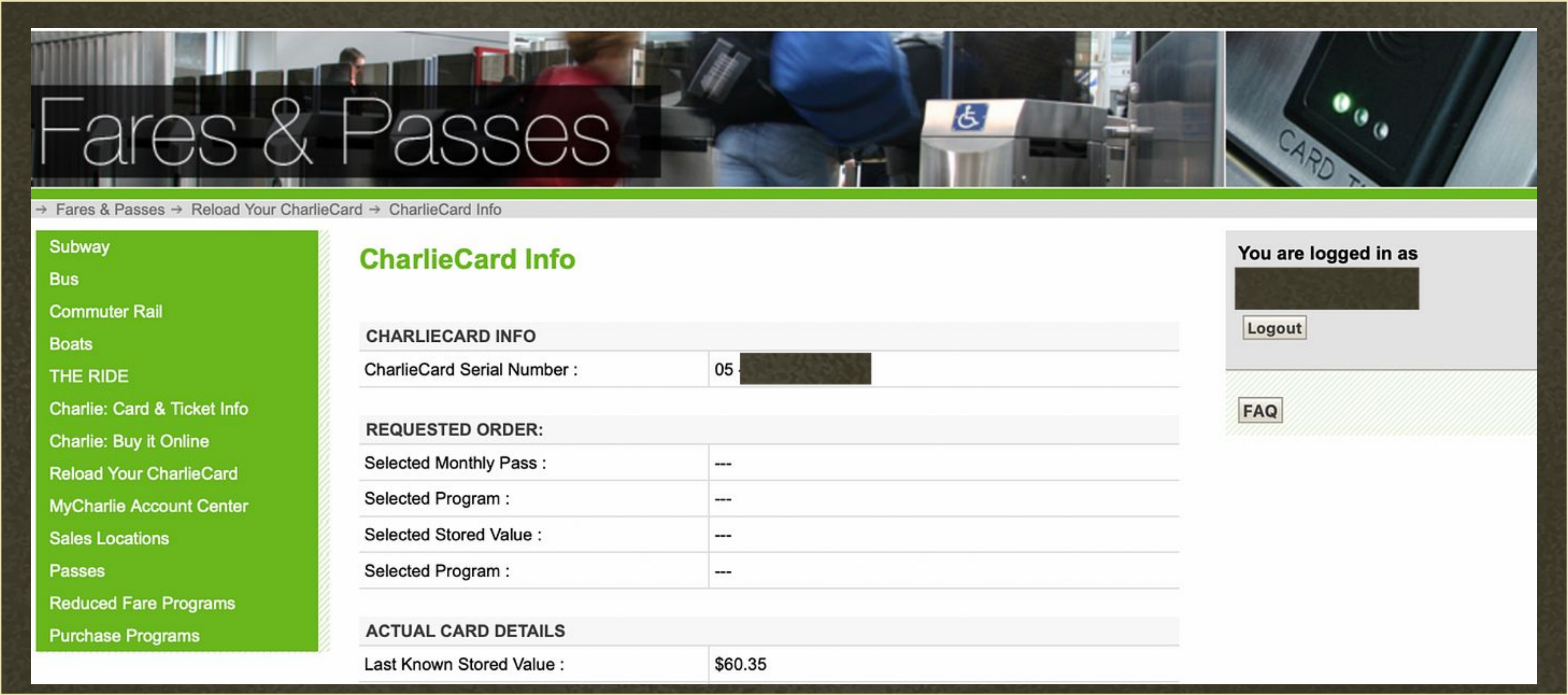
CharlieCard Info

CHARLIECARD INFO	
CharlieCard Serial Number :	05 -[redacted]

REQUESTED ORDER:	
Selected Monthly Pass :	---
Selected Program :	---
Selected Stored Value :	---
Selected Program :	---

ACTUAL CARD DETAILS	
Last Known Stored Value :	$23.60

Online Reloads



[redacted]

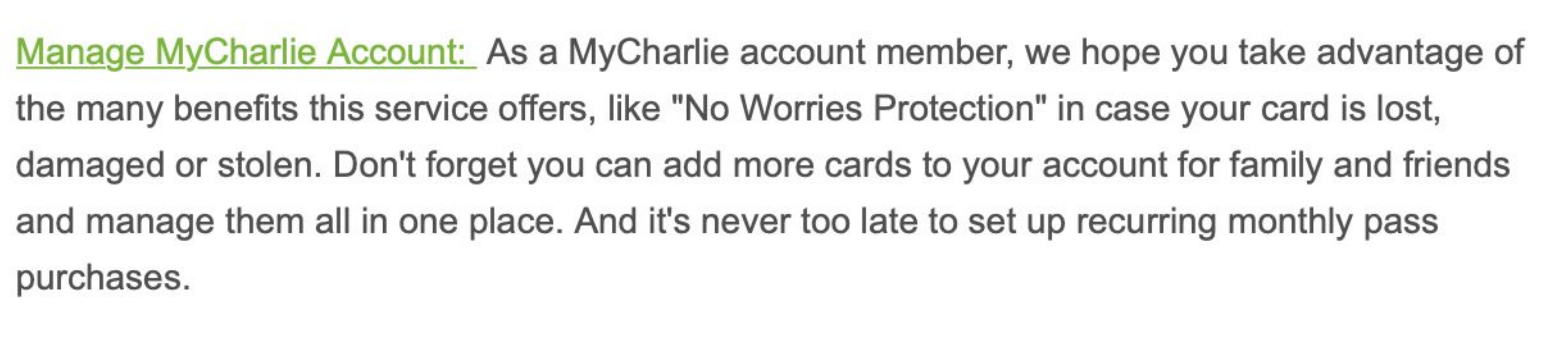
CharlieCard Info

CHARLIECARD INFO	
CharlieCard Serial Number :	05 [redacted]

REQUESTED ORDER:	
Selected Monthly Pass :	---
Selected Program :	---
Selected Stored Value :	---
Selected Program :	---

ACTUAL CARD DETAILS	
Last Known Stored Value :	$60.35

Lost Card



Manage MyCharlie Account: As a MyCharlie account member, we hope you take advantage of the many benefits this service offers, like "No Worries Protection" in case your card is lost, damaged or stolen. Don't forget you can add more cards to your account for family and friends and manage them all in one place. And it's never too late to set up recurring monthly pass purchases.

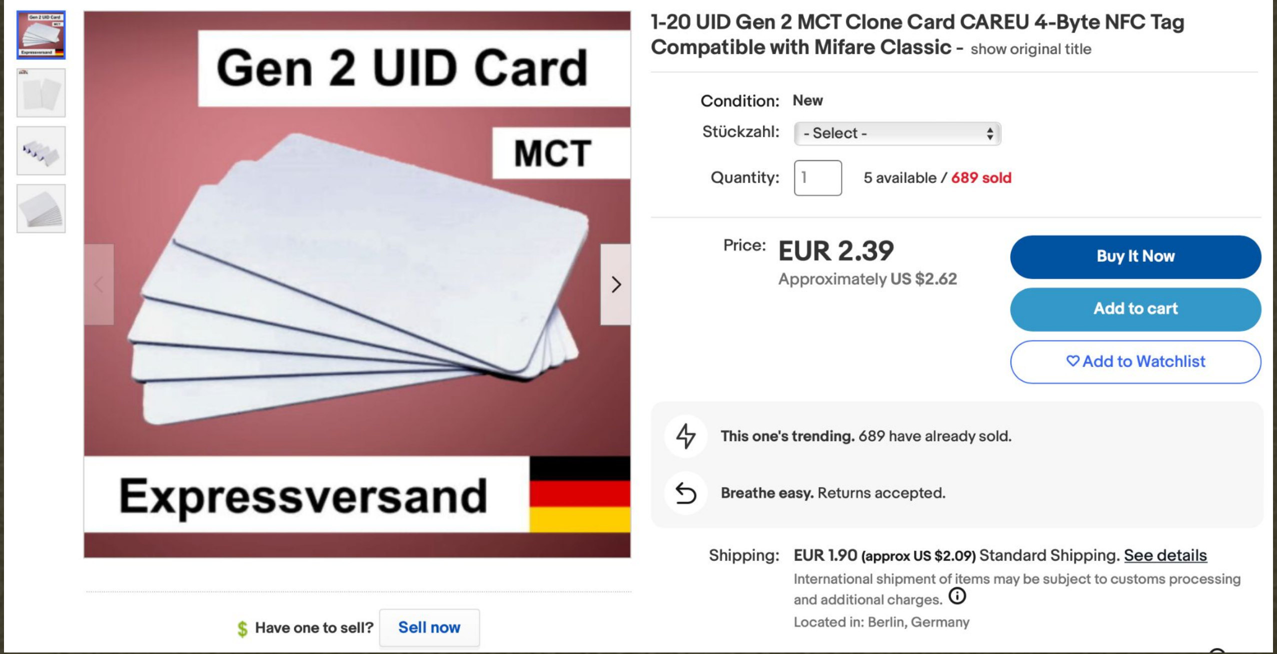
Attack Path #1 - Lost Card

a) Bypasses any ride counter checks

b) Bypasses any “magic” byte checks

c) Bypasses any cryptographic checks

Attack Path #2 - Gen 2 Cards



1-20 UID Gen 2 MCT Clone Card CAREU 4-Byte NFC Tag Compatible with Mifare Classic - show original title

Condition: New

Stückzahl: - Select -

Quantity: 1 5 available / 689 sold

Price: EUR 2.39

Approximately US $2.62

This one's trending. 689 have already sold.

Breathe easy. Returns accepted.

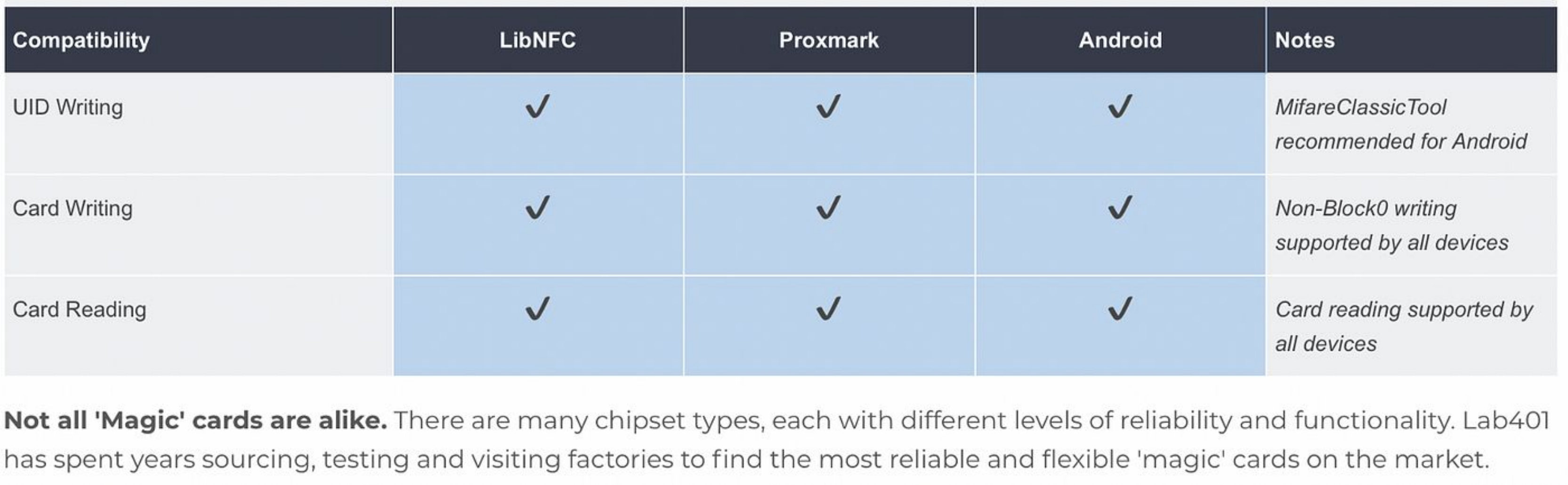
Shipping: EUR 1.90 (approx US $2.09) Standard Shipping. See details

International shipment of items may be subject to customs processing and additional charges.

Located in: Berlin, Germany

$ Have one to sell? Sell now

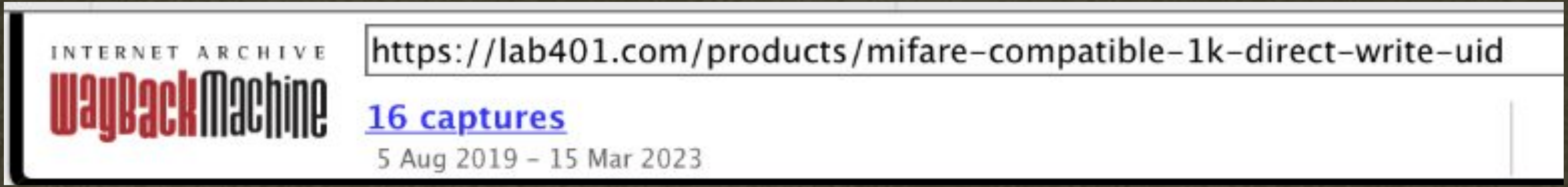
Gen2 Cards



Compatibility	LibNFC	Proxmark	Android	Notes
UID Writing	✓	✓	✓	*MifareClassicTool recommended for Android*
Card Writing	✓	✓	✓	*Non-Block0 writing supported by all devices*
Card Reading	✓	✓	✓	*Card reading supported by all devices*

Not all 'Magic' cards are alike. There are many chipset types, each with different levels of reliability and functionality. Lab401 has spent years sourcing, testing and visiting factories to find the most reliable and flexible 'magic' cards on the market.

Gen2 Cards



https://lab401.com/products/mifare-compatible-1k-direct-write-uid

16 captures

5 Aug 2019 - 15 Mar 2023

Attack Path #3- Rewriting a CharlieCard Snapshot

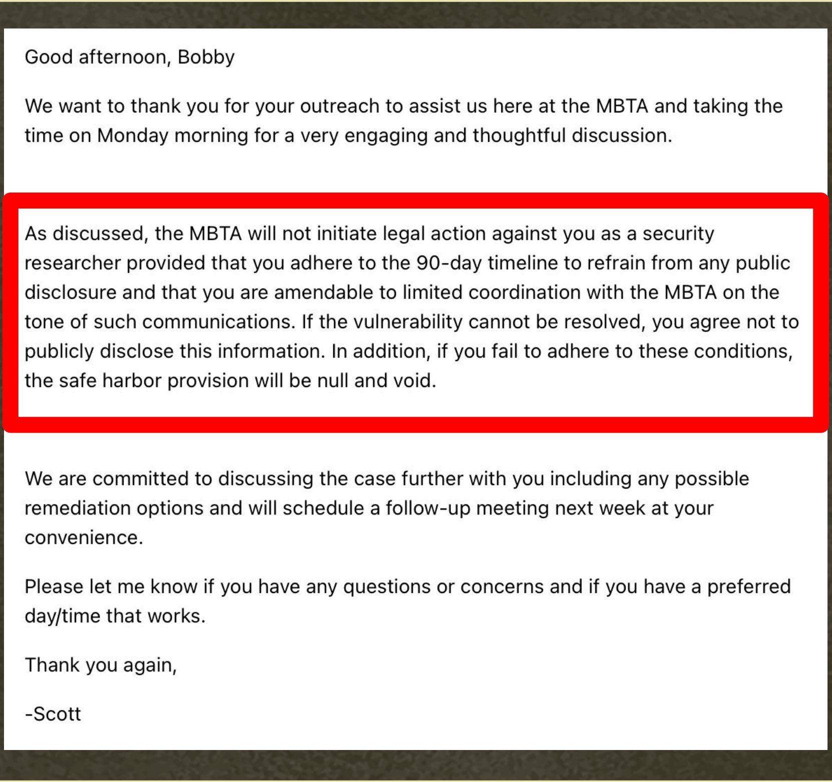
$2.40

$0.00

Covert Disguise

Ride for Free

Vulnerability Disclosure



Good afternoon, Bobby

We want to thank you for your outreach to assist us here at the MBTA and taking the time on Monday morning for a very engaging and thoughtful discussion.

As discussed, the MBTA will not initiate legal action against you as a security researcher provided that you adhere to the 90-day timeline to refrain from any public disclosure and that you are amendable to limited coordination with the MBTA on the tone of such communications. If the vulnerability cannot be resolved, you agree not to publicly disclose this information. In addition, if you fail to adhere to these conditions, the safe harbor provision will be null and void.

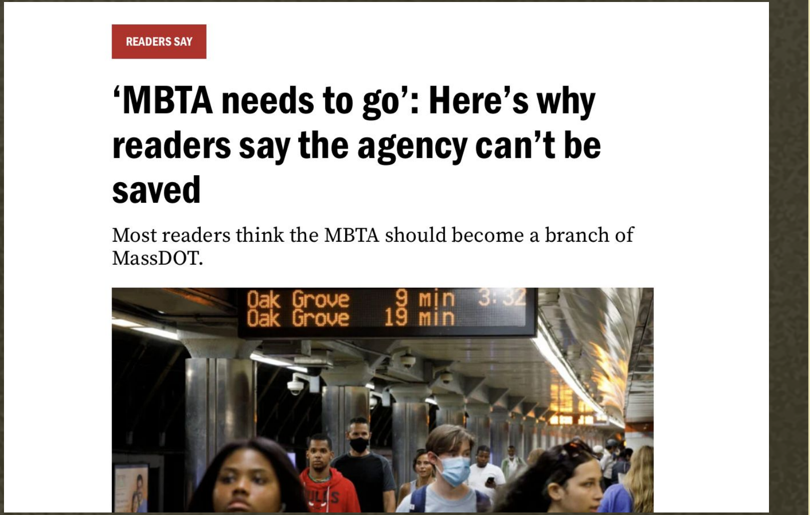
We are committed to discussing the case further with you including any possible remediation options and will schedule a follow-up meeting next week at your convenience.

Please let me know if you have any questions or concerns and if you have a preferred day/time that works.

Thank you again,

-Scott

Potential PR Nightmare?



READERS SAY

‘MBTA needs to go’: Here’s why readers say the agency can’t be saved

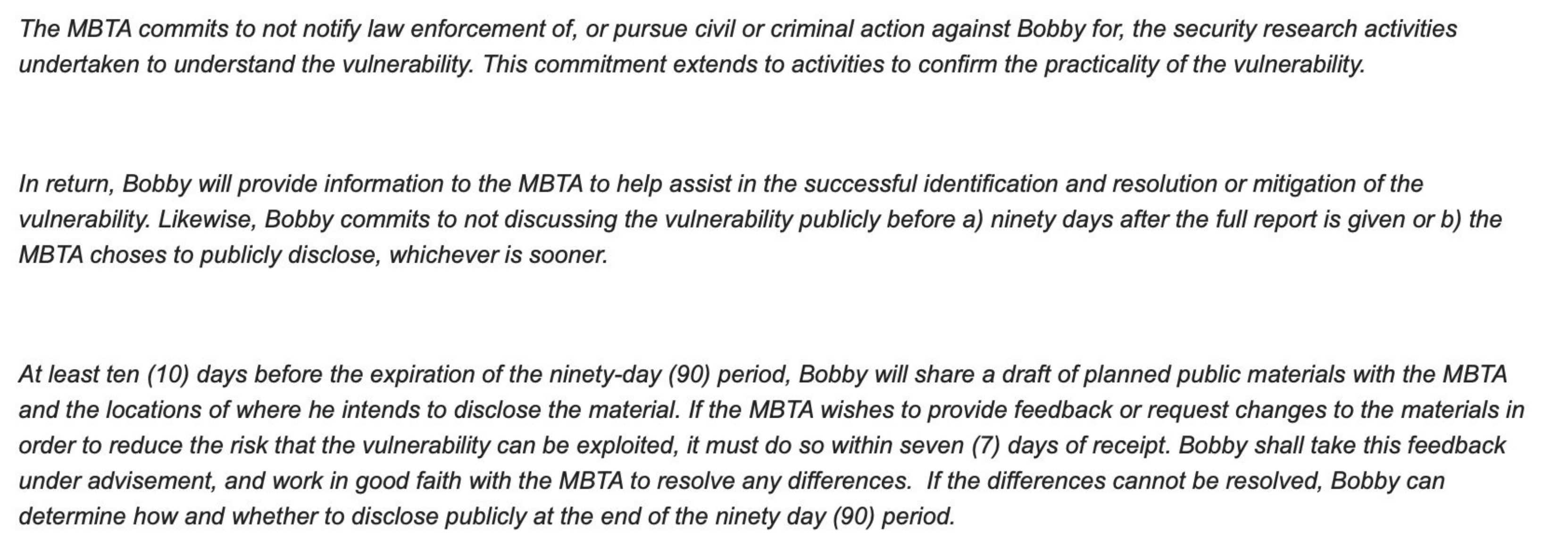
Most readers think the MBTA should become a branch of MassDOT.

Harvard to the Rescue

CYBERLAW CLINIC

HARVARD LAW SCHOOL | BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY

Vulnerability Disclosure

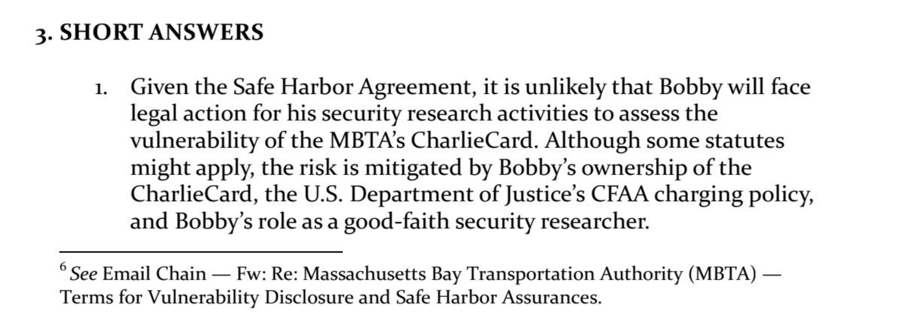


The MBTA commits to not notify law enforcement of, or pursue civil or criminal action against Bobby for, the security research activities undertaken to understand the vulnerability. This commitment extends to activities to confirm the practicality of the vulnerability.

In return, Bobby will provide information to the MBTA to help assist in the successful identification and resolution or mitigation of the vulnerability. Likewise, Bobby commits to not discussing the vulnerability publicly before a) ninety days after the full report is given or b) the MBTA choses to publicly disclose, whichever is sooner.

At least ten (10) days before the expiration of the ninety-day (90) period, Bobby will share a draft of planned public materials with the MBTA and the locations of where he intends to disclose the material. If the MBTA wishes to provide feedback or request changes to the materials in order to reduce the risk that the vulnerability can be exploited, it must do so within seven (7) days of receipt. Bobby shall take this feedback under advisement, and work in good faith with the MBTA to resolve any differences. If the differences cannot be resolved, Bobby can determine how and whether to disclose publicly at the end of the ninety day (90) period.

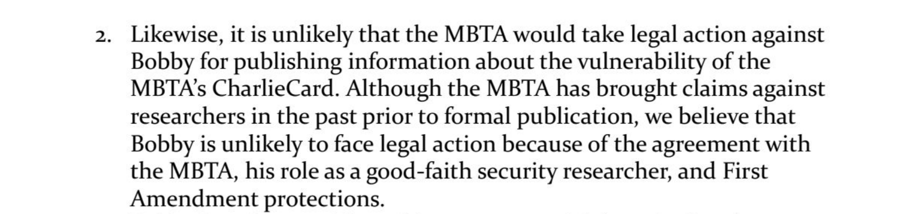
Harvard to the Rescue



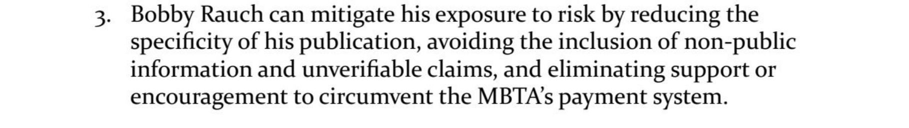
3. SHORT ANSWERS

1. Given the Safe Harbor Agreement, it is unlikely that Bobby will face legal action for his security research activities to assess the vulnerability of the MBTA's CharlieCard. Although some statutes might apply, the risk is mitigated by Bobby's ownership of the CharlieCard, the U.S. Department of Justice's CFAA charging policy, and Bobby's role as a good-faith security researcher.

[6] *See* Email Chain — Fw: Re: Massachusetts Bay Transportation Authority (MBTA) — Terms for Vulnerability Disclosure and Safe Harbor Assurances.



2. Likewise, it is unlikely that the MBTA would take legal action against Bobby for publishing information about the vulnerability of the MBTA's CharlieCard. Although the MBTA has brought claims against researchers in the past prior to formal publication, we believe that Bobby is unlikely to face legal action because of the agreement with the MBTA, his role as a good-faith security researcher, and First Amendment protections.



3. Bobby Rauch can mitigate his exposure to risk by reducing the specificity of his publication, avoiding the inclusion of non-public information and unverifiable claims, and eliminating support or encouragement to circumvent the MBTA's payment system.

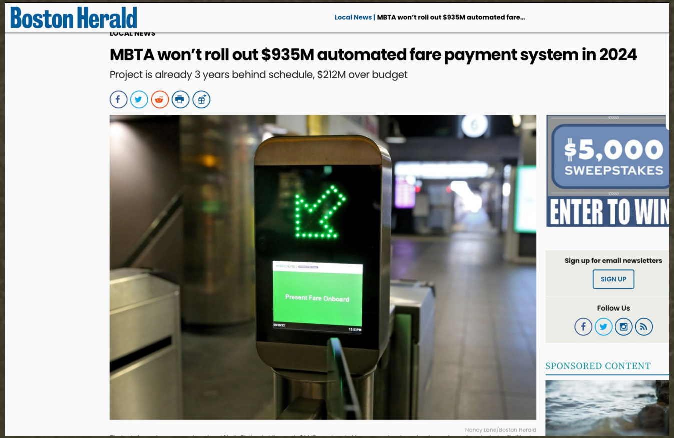
Suggested Remediations

1. Server-side validation and tracking of card values
2. Tie value increases on the card with associated refill transactions
3. As CharlieCards get tapped against fare vending machines, regularly change the encryption keys, so they are different across cards, and subsequently regularly rotate them on a scheduled basis
4. Upgrade to a more secure Mifare technology like Mifare DESFire

Actual Remediations

1. “Improved system monitoring efforts for fraudulent rides”

2. Increased headcount of personnel dedicated to this system monitoring



Boston Herald

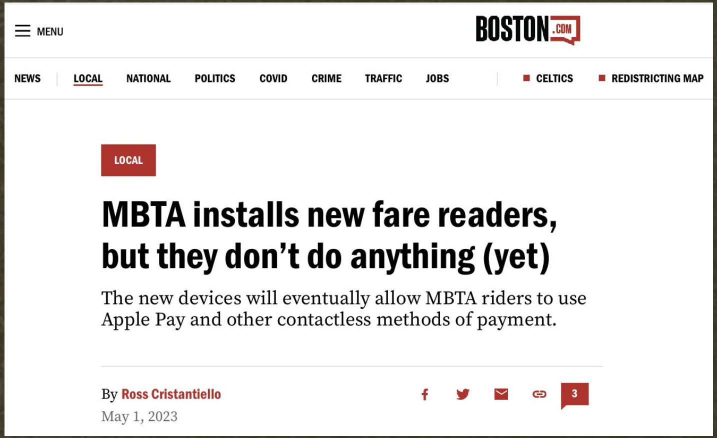
Local News | MBTA won’t roll out $935M automated fare...

LOCAL NEWS

MBTA won’t roll out $935M automated fare payment system in 2024

Project is already 3 years behind schedule, $212M over budget

Nancy Lane/Boston Herald



BOSTON.COM

LOCAL

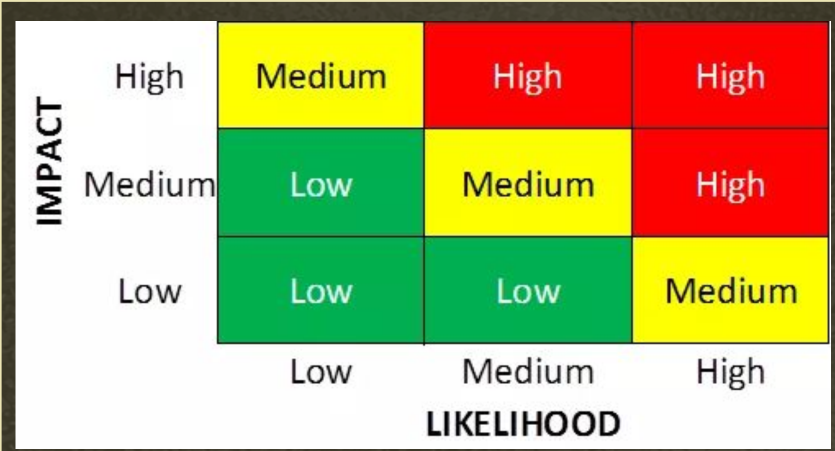
MBTA installs new fare readers, but they don’t do anything (yet)

The new devices will eventually allow MBTA riders to use Apple Pay and other contactless methods of payment.

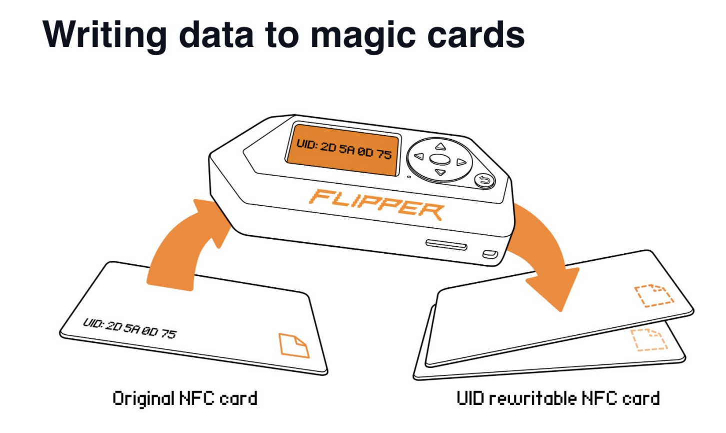
By Ross Cristantiello

May 1, 2023

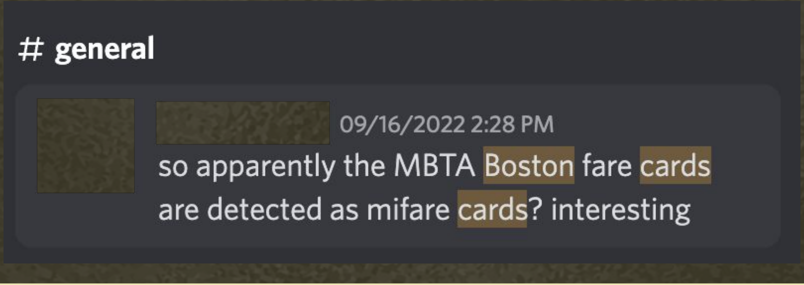
Closing Thoughts



IMPACT			
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium
	Low	Medium	High
		LIKELIHOOD	



Writing data to magic cards



general

[redacted] [redacted] 09/16/2022 2:28 PM

so apparently the MBTA Boston fare cards are detected as mifare cards? interesting

THANKS!

Questions?

Bobbyrsec.com
Twitter.com/bobbyrsec
LinkedIn.com/in/bobby-rauch/

CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon, and infographics & images by Freepik