Exploiting Passbook

Who am I?

- Undergraduate Computer Science Student
- Software Developer
- Vulnerability Researcher
- @DaKnObCS

Disclaimer

All the content in this presentation is entirely hypothetical. Any similarity with real life people, companies, situations or places is entirely coincidental. What you are about to see is my work and I am not endorsed or affiliated by any third party, individual or company. I take no responsibility for your actions should you attempt any of this stuff.

What is passbook?

Passbook keeps things like airline boarding passes, movie tickets, and gift cards all in one place, letting you scan your iPhone or iPod touch to check in for a flight, get into a movie, redeem a coupon, and more.

What is this all about?

- Easy ways to forge a valid Passbook Boarding Pass
  - No technical knowledge required
  - Can be done in a Chrome Book
- Get past the Security Checkpoint
  - As long as you don’t carry any guns
  - Or luggage ;(
- Get into an airplane

What you'll need

iPhone
With Passbook

Web Browser
Obviously not IE

Photo Editor
Any editor will do

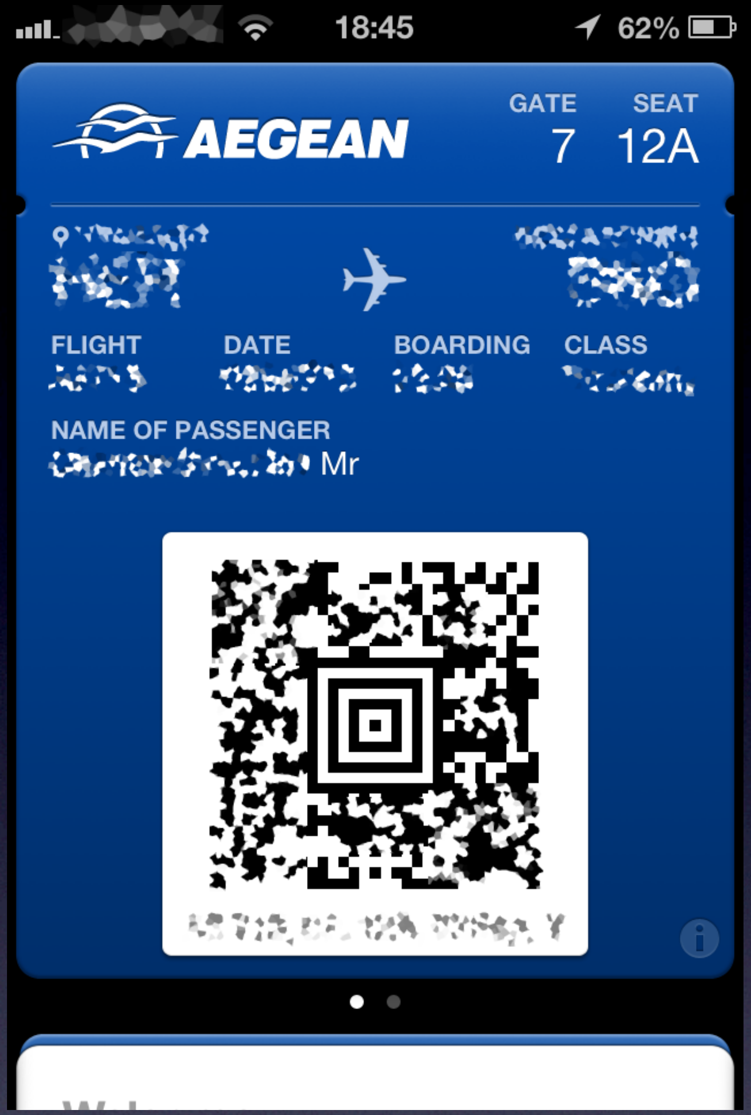
Balls
A pair should do

The iPhone and the Safari are trademarks of Apple, Inc. The Photoshop icon is a trademark of Adobe. All rights to their respective owners.

STEP 1:

Find screenshots of an original boarding pass or use some you might have from previous trips.

(The more the better)



[redacted] 18:45 62%

AEGEAN

GATE 7

SEAT 12A

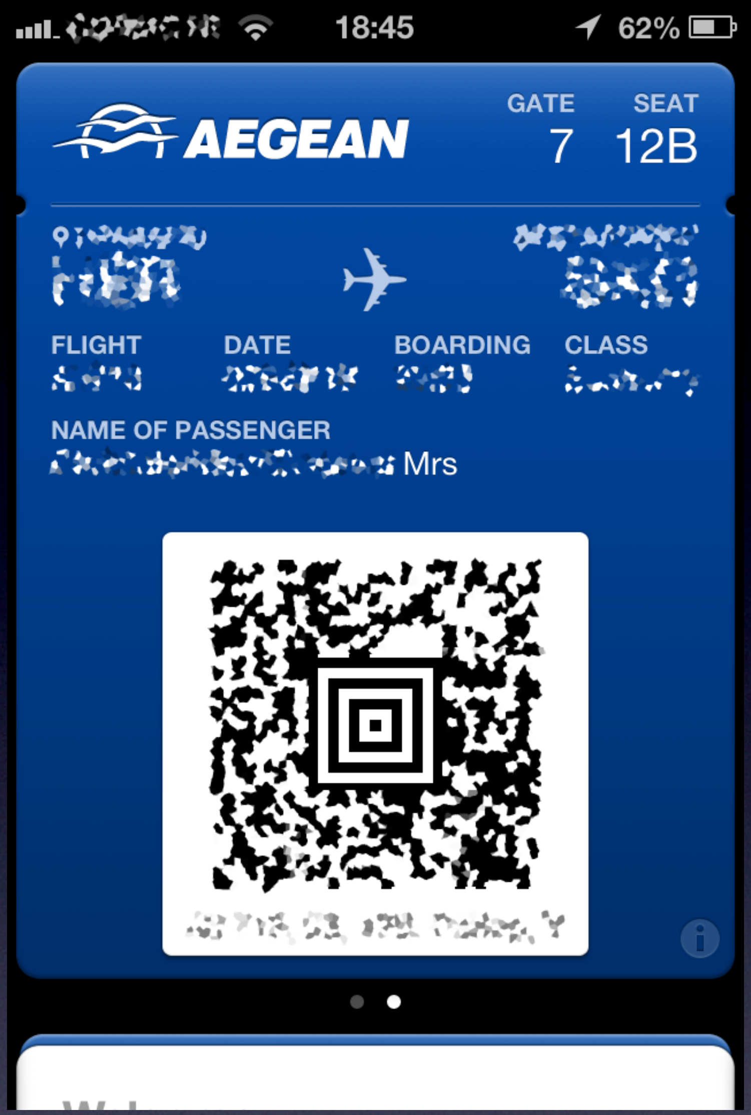
[redacted]

FLIGHT	DATE	BOARDING	CLASS
[redacted]	[redacted]	[redacted]	[redacted]

NAME OF PASSENGER

[redacted] Mr

[redacted]



[redacted] 18:45 62%

AEGEAN

GATE 7

SEAT 12B

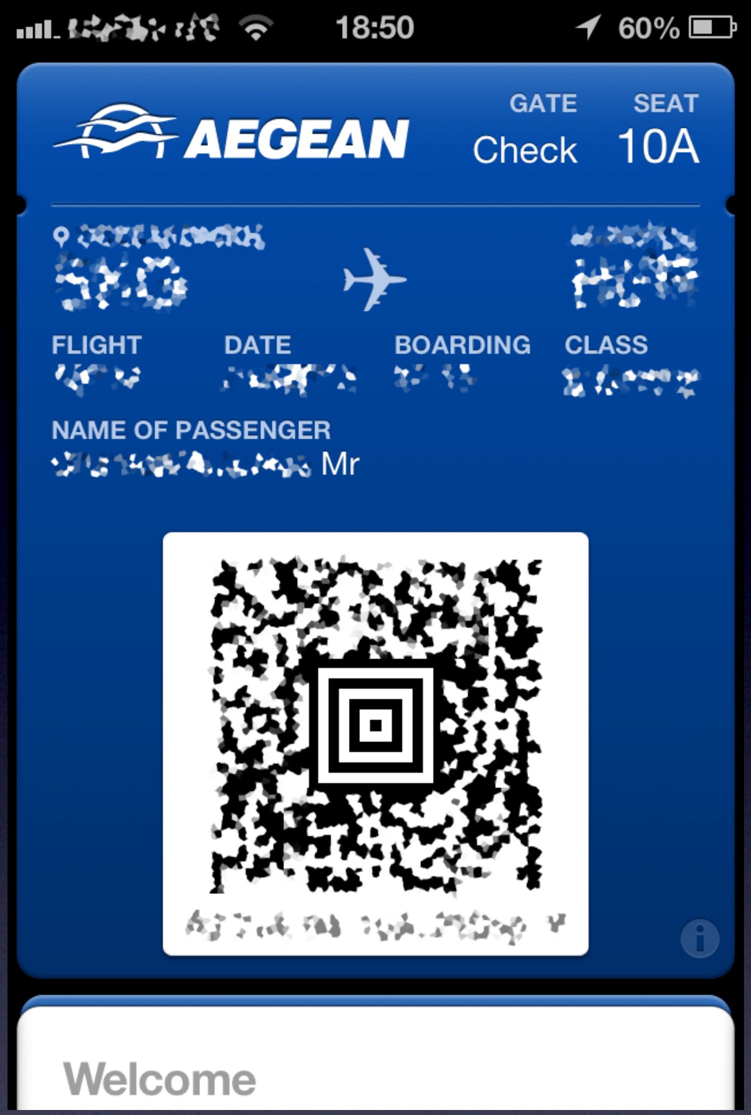
[redacted]

FLIGHT	DATE	BOARDING	CLASS
[redacted]	[redacted]	[redacted]	[redacted]

NAME OF PASSENGER

[redacted] Mrs

[redacted]



[redacted] 18:50 60%

AEGEAN

GATE Check

SEAT 10A

[redacted]

FLIGHT	DATE	BOARDING	CLASS
[redacted]	[redacted]	[redacted]	[redacted]

NAME OF PASSENGER

[redacted] Mr

[redacted]

Welcome

Three valid passes

I was lucky to have those. If you aren’t, search on Bing

or Google :)

STEP 2:

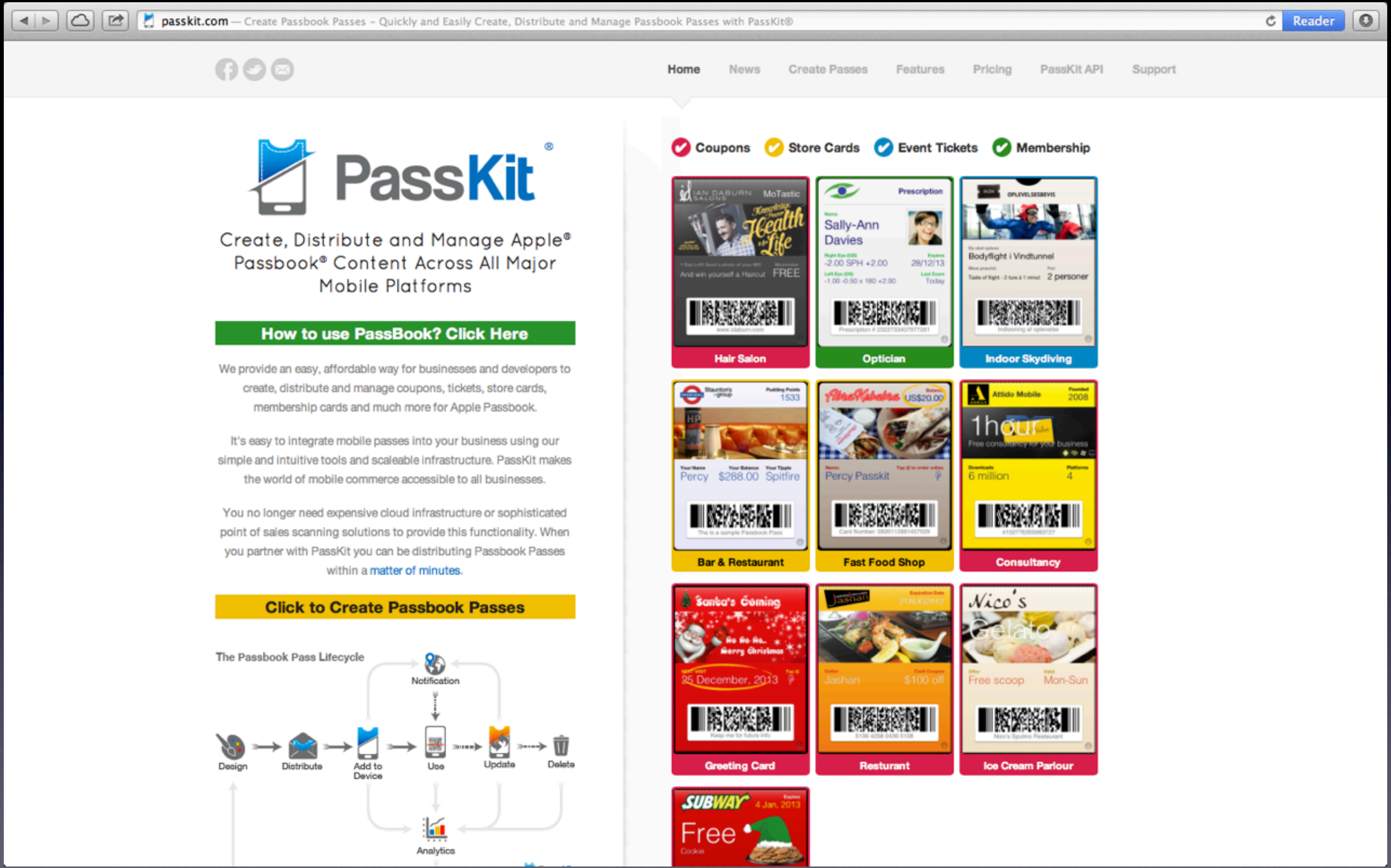
Use a WYSIWYG online service or Apple’s PassKit if you’re an enrolled developer to make an identically looking pass.

(It doesn’t have to be perfect)

Now let's assume there's a website called

PassKit

and it looks like this...

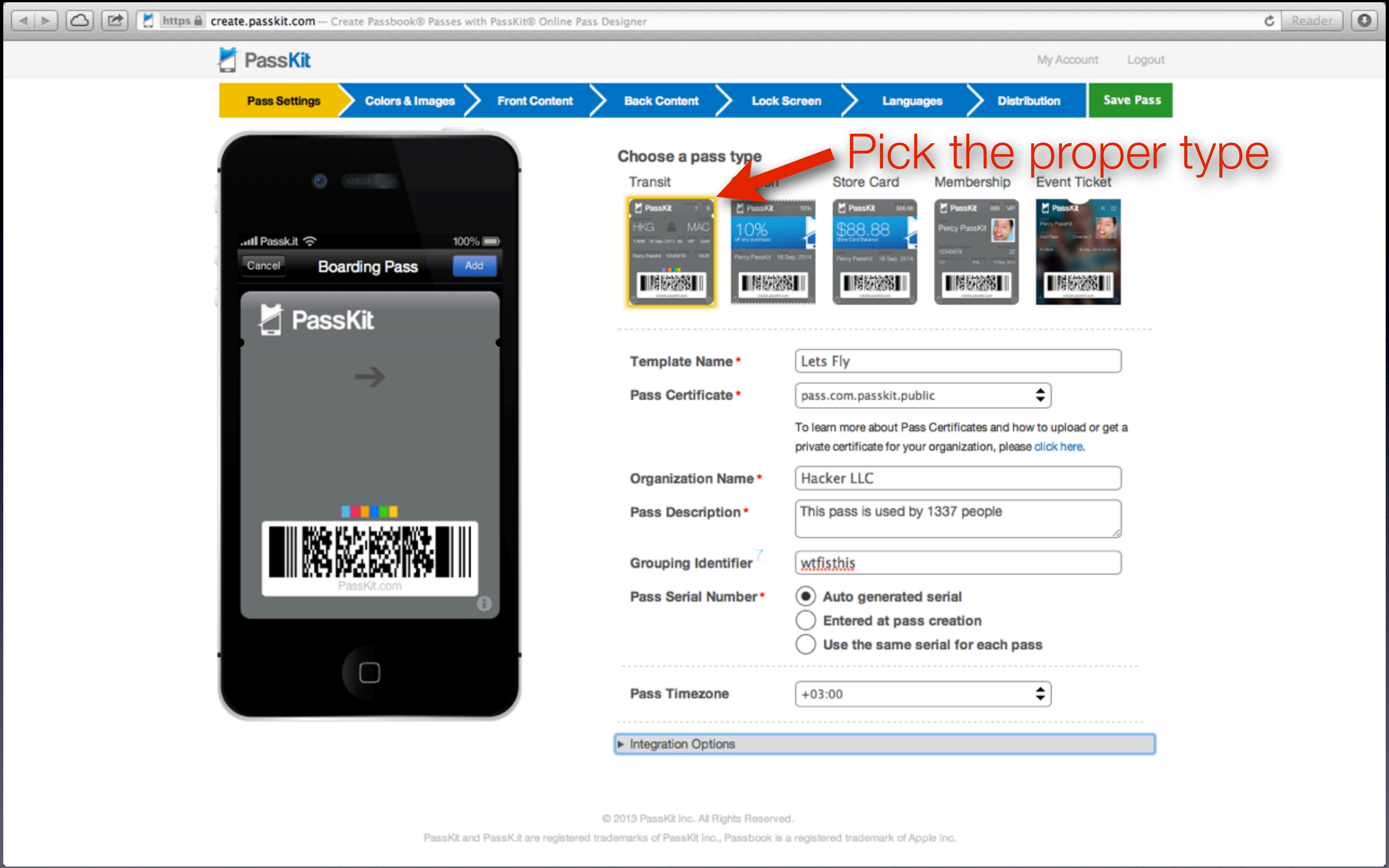


Create, Distribute and Manage Apple® Passbook® Content Across All Major Mobile Platforms

We provide an easy, affordable way for businesses and developers to create, distribute and manage coupons, tickets, store cards, membership cards and much more for Apple Passbook.

It's easy to integrate mobile passes into your business using our simple and intuitive tools and scaleable infrastructure. PassKit makes the world of mobile commerce accessible to all businesses.

You no longer need expensive cloud infrastructure or sophisticated point of sales scanning solutions to provide this functionality. When you partner with PassKit you can be distributing Passbook Passes within a matter of minutes.



Pick the proper type

Choose a pass type

Transit | ...on | Store Card | Membership | Event Ticket

Template Name* Lets Fly

Pass Certificate* pass.com.passkit.public

To learn more about Pass Certificates and how to upload or get a private certificate for your organization, please click here.

Organization Name* Hacker LLC

Pass Description* This pass is used by 1337 people

Grouping Identifier wtfisthis

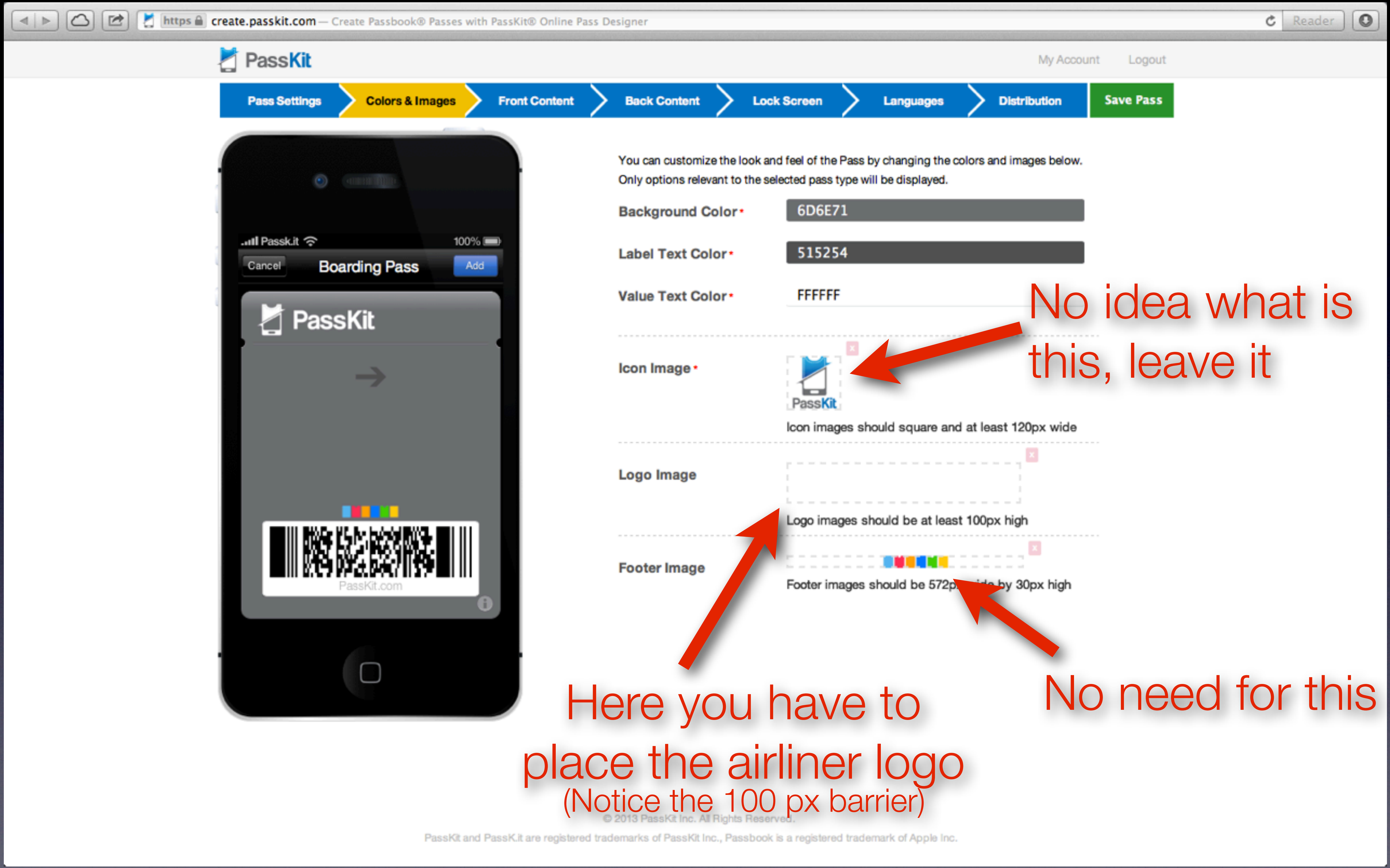
Pass Serial Number*
● Auto generated serial
○ Entered at pass creation
○ Use the same serial for each pass

Pass Timezone +03:00

▸ Integration Options

© 2013 PassKit Inc. All Rights Reserved.

PassKit and PassKit are registered trademarks of PassKit Inc., Passbook is a registered trademark of Apple Inc.



You can customize the look and feel of the Pass by changing the colors and images below. Only options relevant to the selected pass type will be displayed.

Background Color• 6D6E71

Label Text Color• 515254

Value Text Color• FFFFFF

Icon Image•

Icon images should square and at least 120px wide

Logo Image

Logo images should be at least 100px high

Footer Image

Footer images should be 572px wide by 30px high

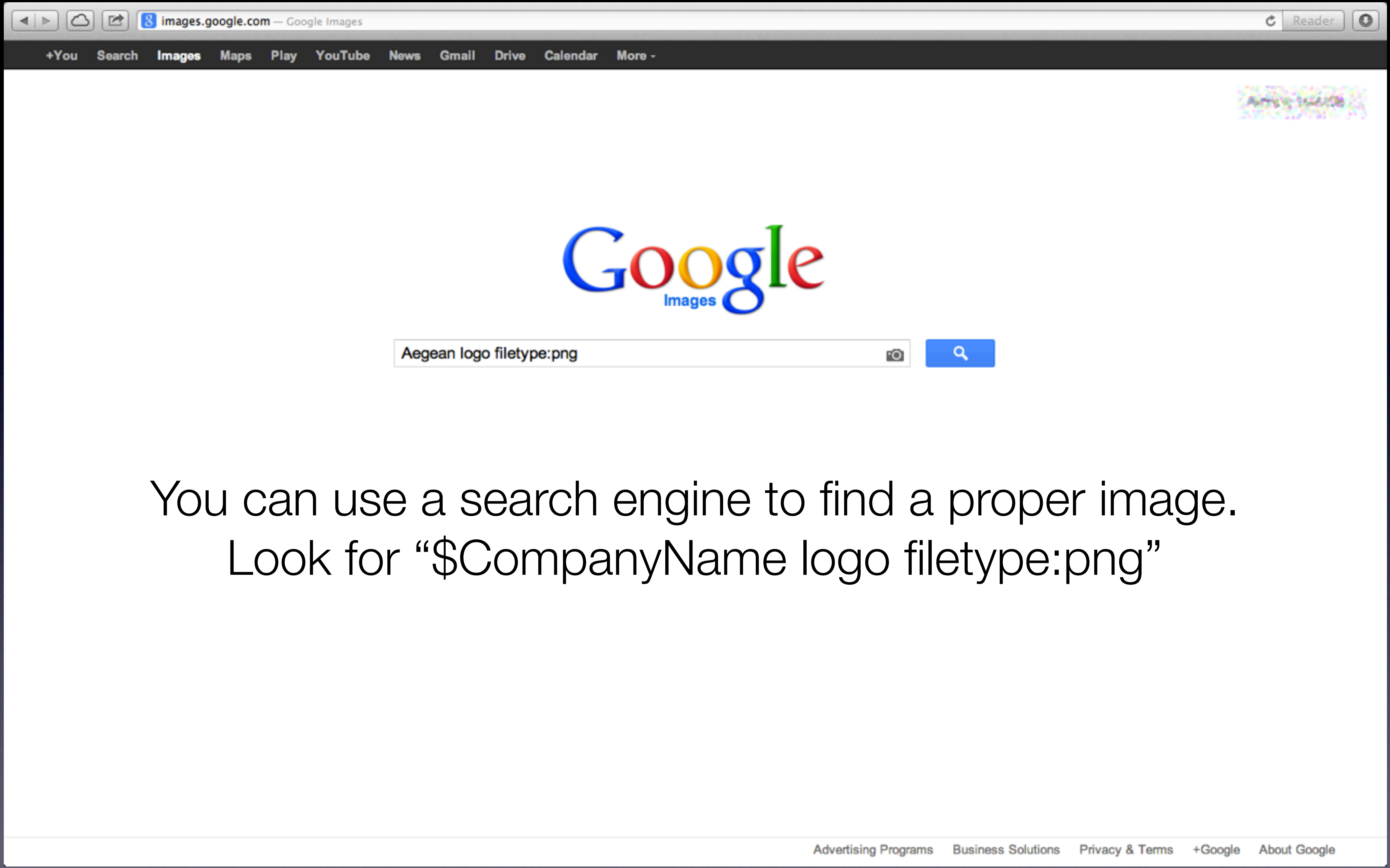
No idea what is this, leave it

Here you have to place the airliner logo (Notice the 100 px barrier)

No need for this

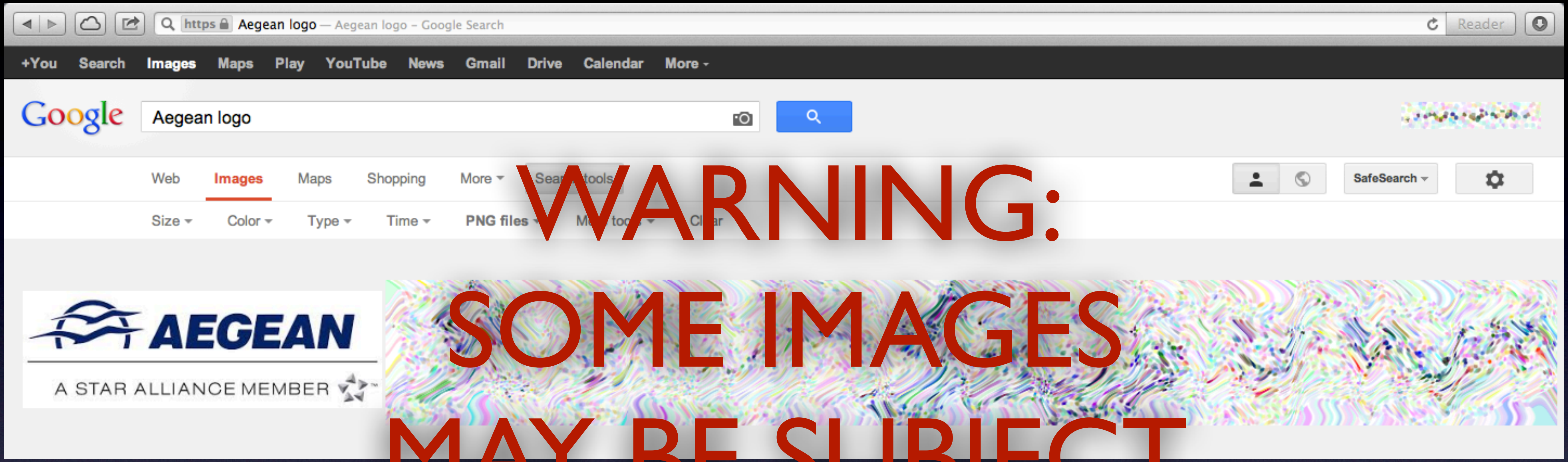
© 2013 PassKit Inc. All Rights Reserved.

PassKit and PassKit are registered trademarks of PassKit Inc., Passbook is a registered trademark of Apple Inc.



Aegean logo filetype:png

You can use a search engine to find a proper image.
Look for “$CompanyName logo filetype:png”



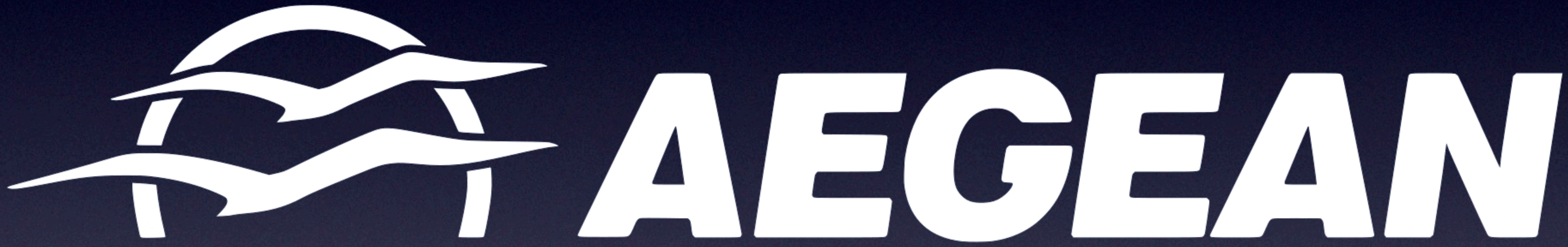
Aegean logo

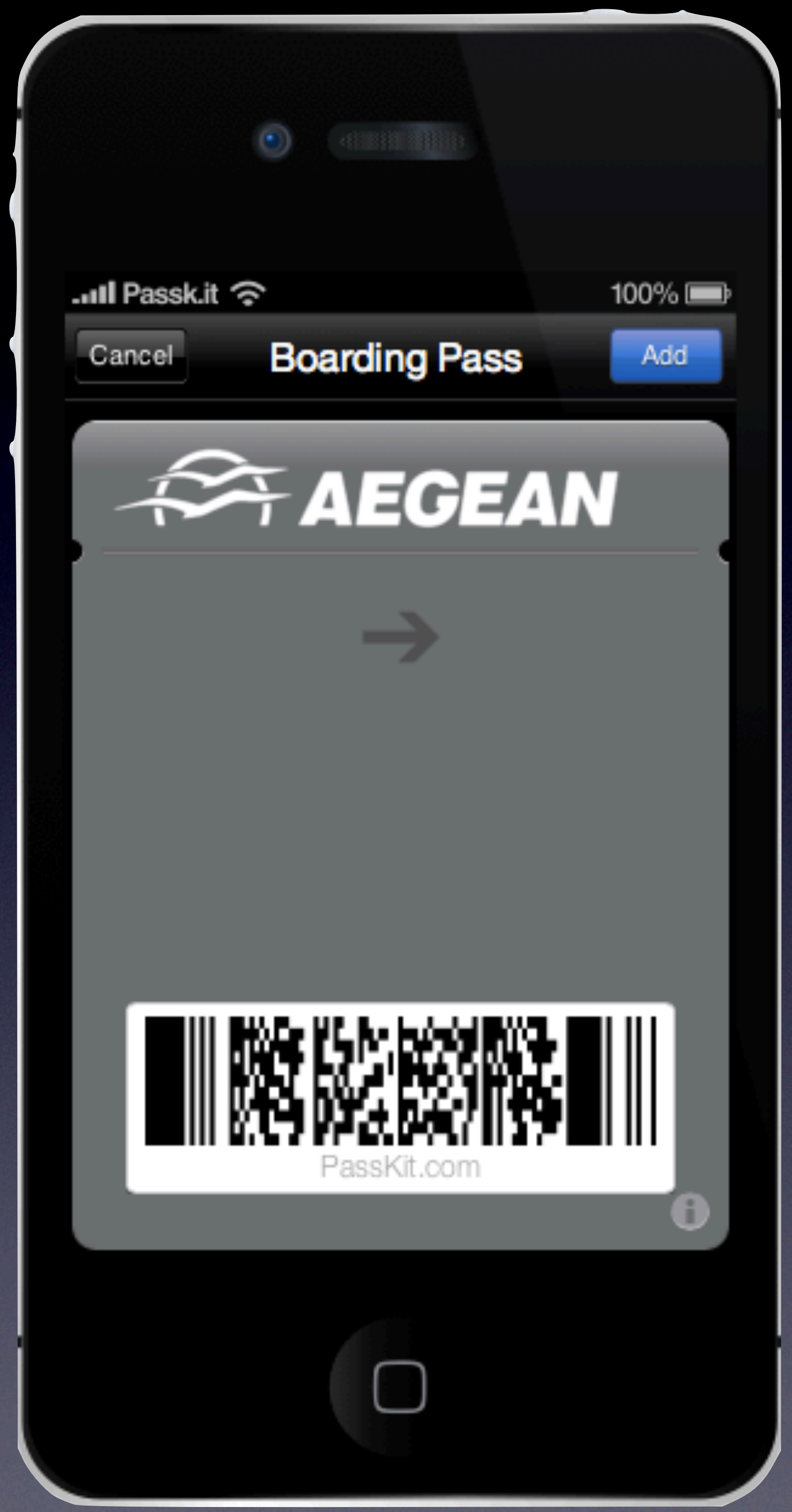
WARNING: SOME IMAGES MAY BE SUBJECT TO COPYRIGHT

Now locate a logo that looks like the one in the Passbook. It doesn't matter if it is the same color or size, you can always resize it, paint it and crop it later.

Keep in mind: The bigger resolution the better

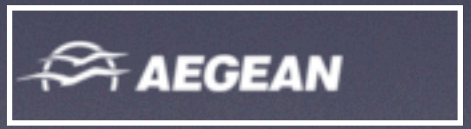
If your image editing skills are decent, you will come to something like this here:



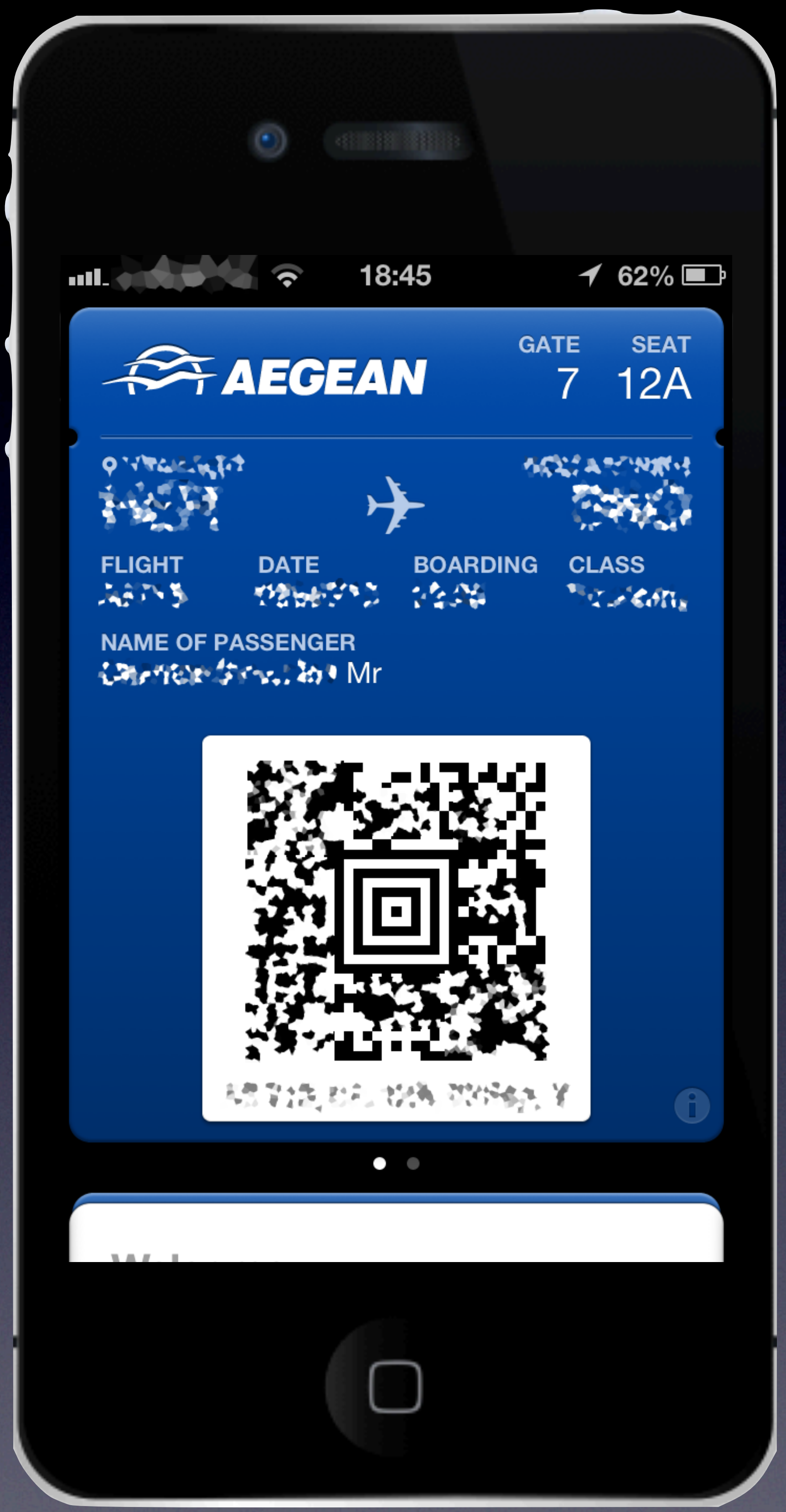


But this is not quite identical, now is it?

You need to pad the logo within the image. I ended up using the following one.



(Without the border)



GATE 7

SEAT 12A

[redacted] [redacted]

FLIGHT [redacted]

DATE [redacted]

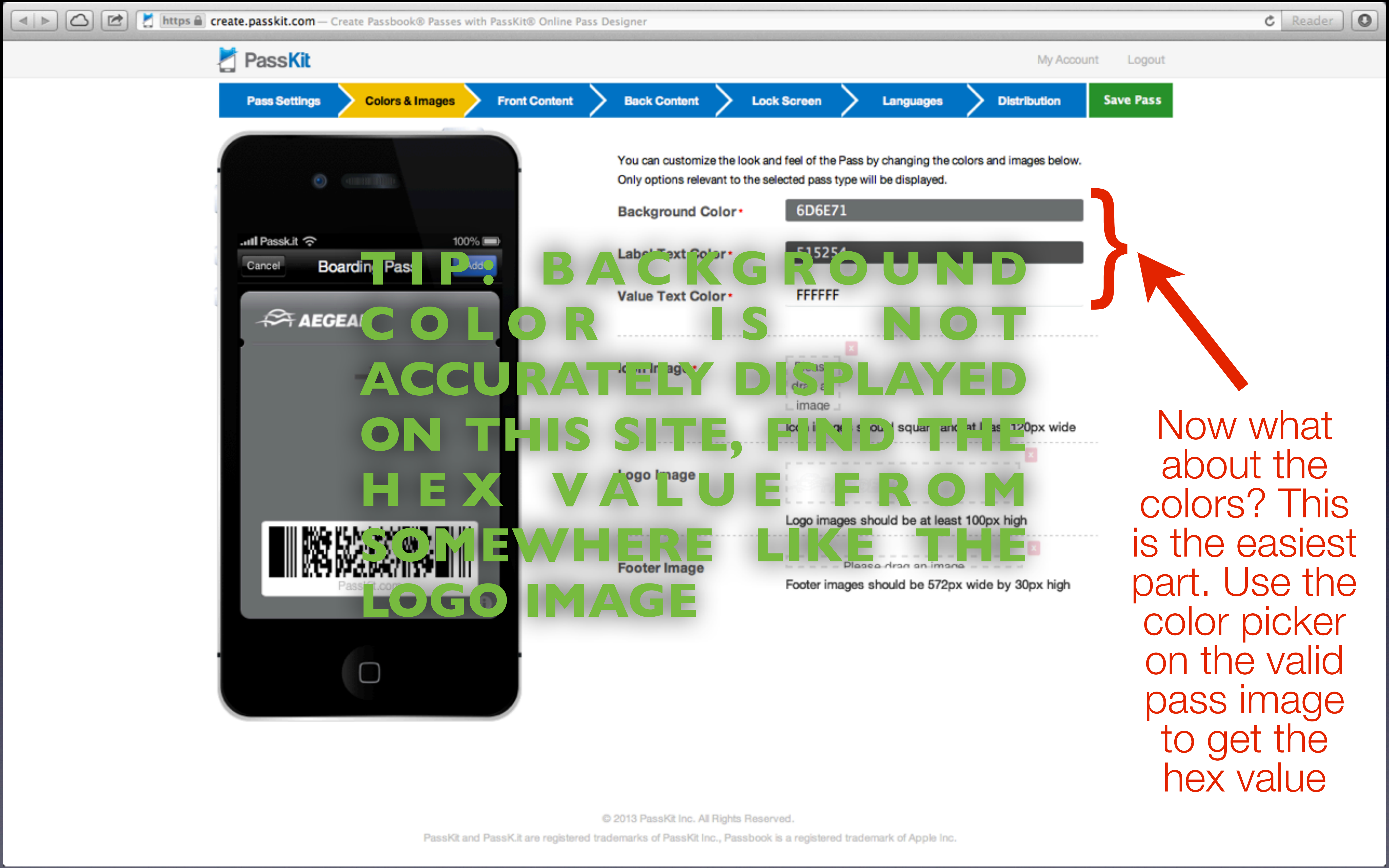
BOARDING [redacted]

CLASS [redacted]

NAME OF PASSENGER

[redacted] Mr

[redacted]



You can customize the look and feel of the Pass by changing the colors and images below.
Only options relevant to the selected pass type will be displayed.

Background Color* 6D6E71

Label Text Color* 515254

Value Text Color* FFFFFF

Icon Image*

Icon images should be square and at least 120px wide

Logo Image

Logo images should be at least 100px high

Footer Image

Please drag an image

Footer images should be 572px wide by 30px high

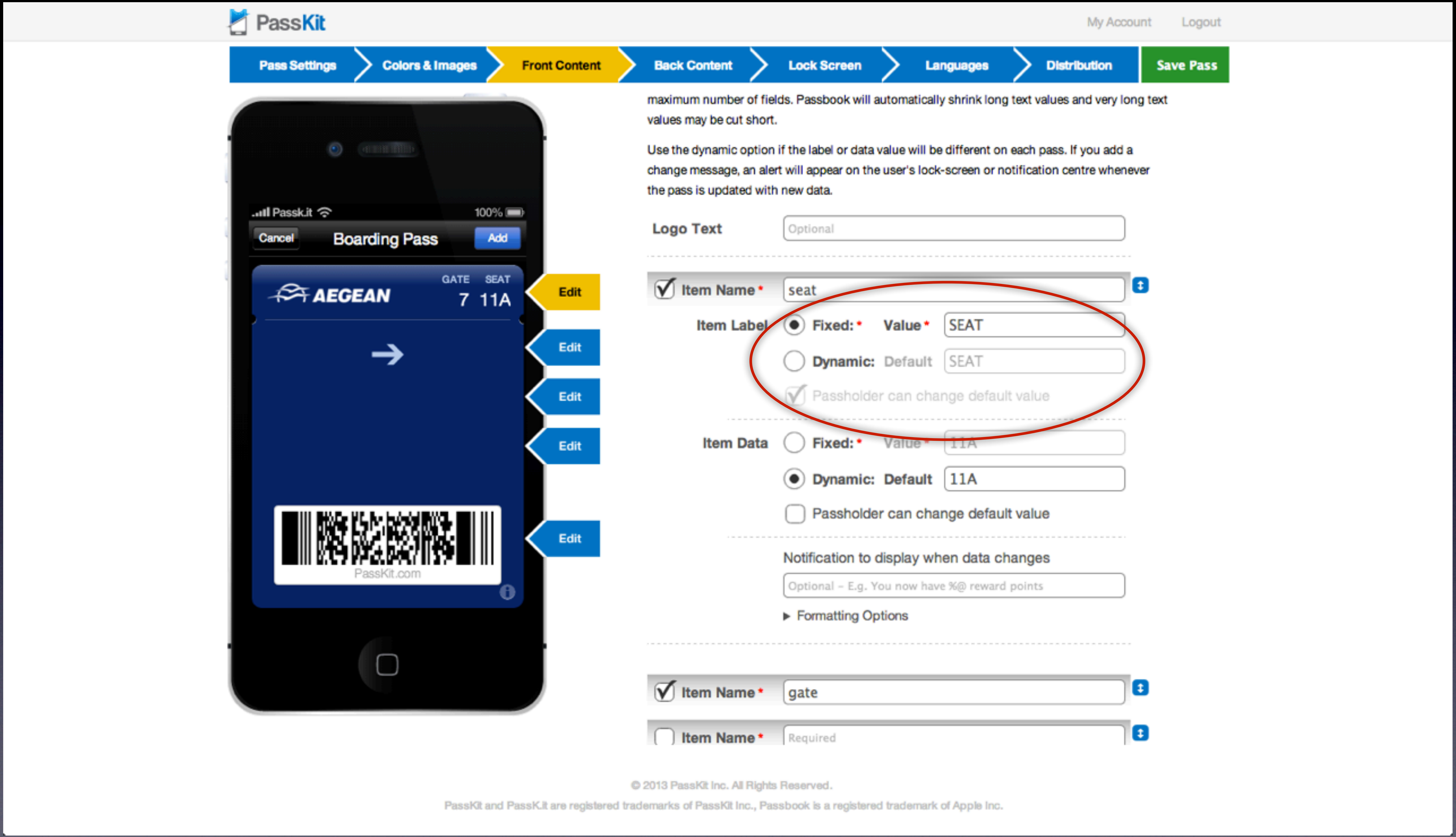
© 2013 PassKit Inc. All Rights Reserved.

PassKit and PassK.it are registered trademarks of PassKit Inc., Passbook is a registered trademark of Apple Inc.

TIP: BACKGROUND COLOR IS NOT ACCURATELY DISPLAYED ON THIS SITE, FIND THE HEX VALUE FROM SOMEWHERE LIKE THE LOGO IMAGE

Now what about the colors? This is the easiest part. Use the color picker on the valid pass image to get the hex value

© AEGEAN AIRLINES S.A. - Use under Directive 2001/29/EC



maximum number of fields. Passbook will automatically shrink long text values and very long text values may be cut short.

Use the dynamic option if the label or data value will be different on each pass. If you add a change message, an alert will appear on the user's lock-screen or notification centre whenever the pass is updated with new data.

Logo Text: Optional

☑ Item Name*: seat

Item Label: ● Fixed:* Value* SEAT
○ Dynamic: Default SEAT
☑ Passholder can change default value

Item Data: ○ Fixed:* Value* 11A
● Dynamic: Default 11A
□ Passholder can change default value

Notification to display when data changes: Optional – E.g. You now have %@ reward points

▸ Formatting Options

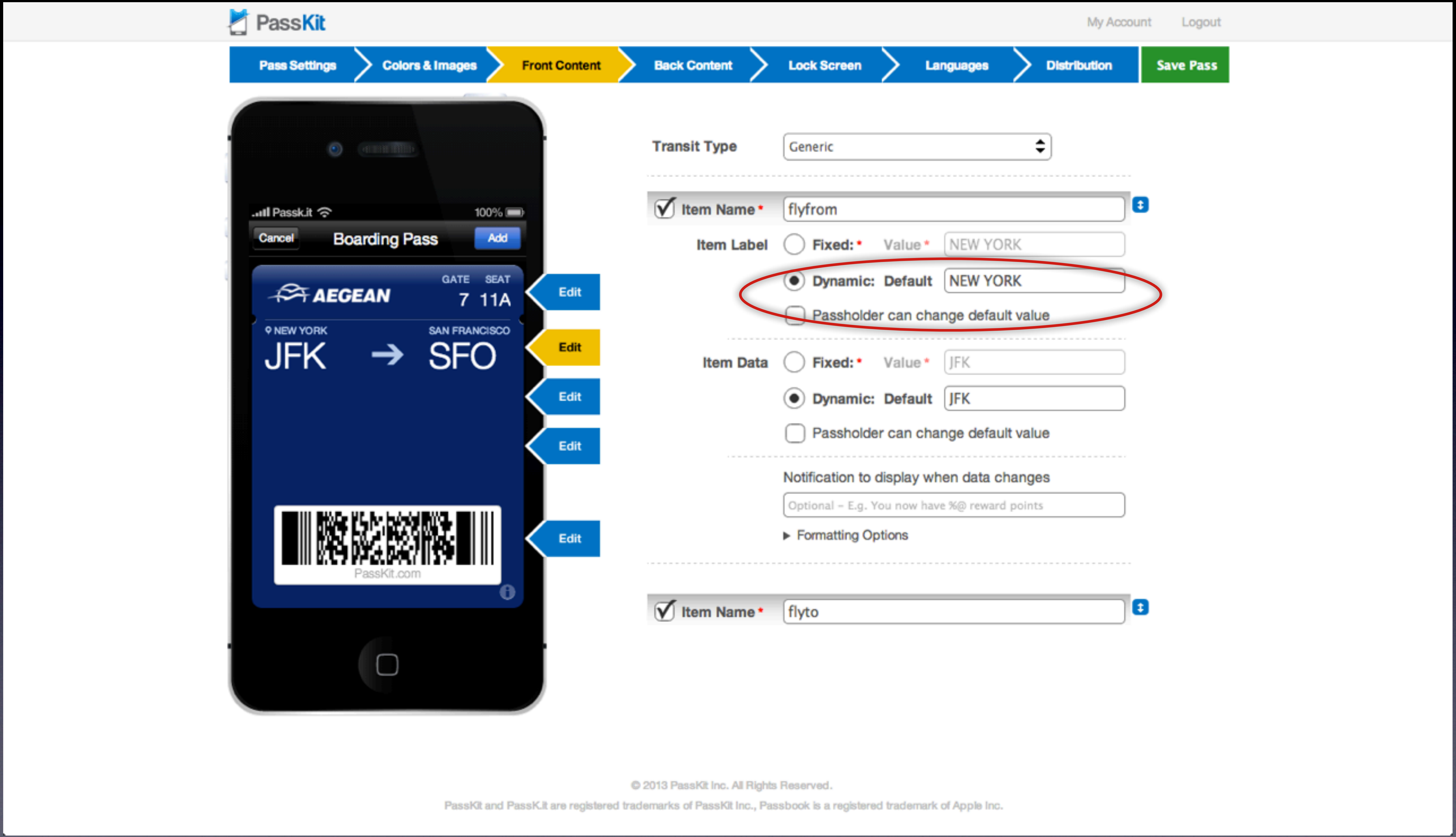
☑ Item Name*: gate

□ Item Name*: Required

© 2013 PassKit Inc. All Rights Reserved.

PassKit and PassK.it are registered trademarks of PassKit Inc., Passbook is a registered trademark of Apple Inc.

© AEGEAN AIRLINES S.A. - Use under Directive 2001/29/EC



Transit Type: Generic

☑ Item Name*: flyfrom

Item Label
○ Fixed:* Value* NEW YORK
● Dynamic: Default NEW YORK
□ Passholder can change default value

Item Data
○ Fixed:* Value* JFK
● Dynamic: Default JFK
□ Passholder can change default value

Notification to display when data changes: Optional – E.g. You now have %@ reward points

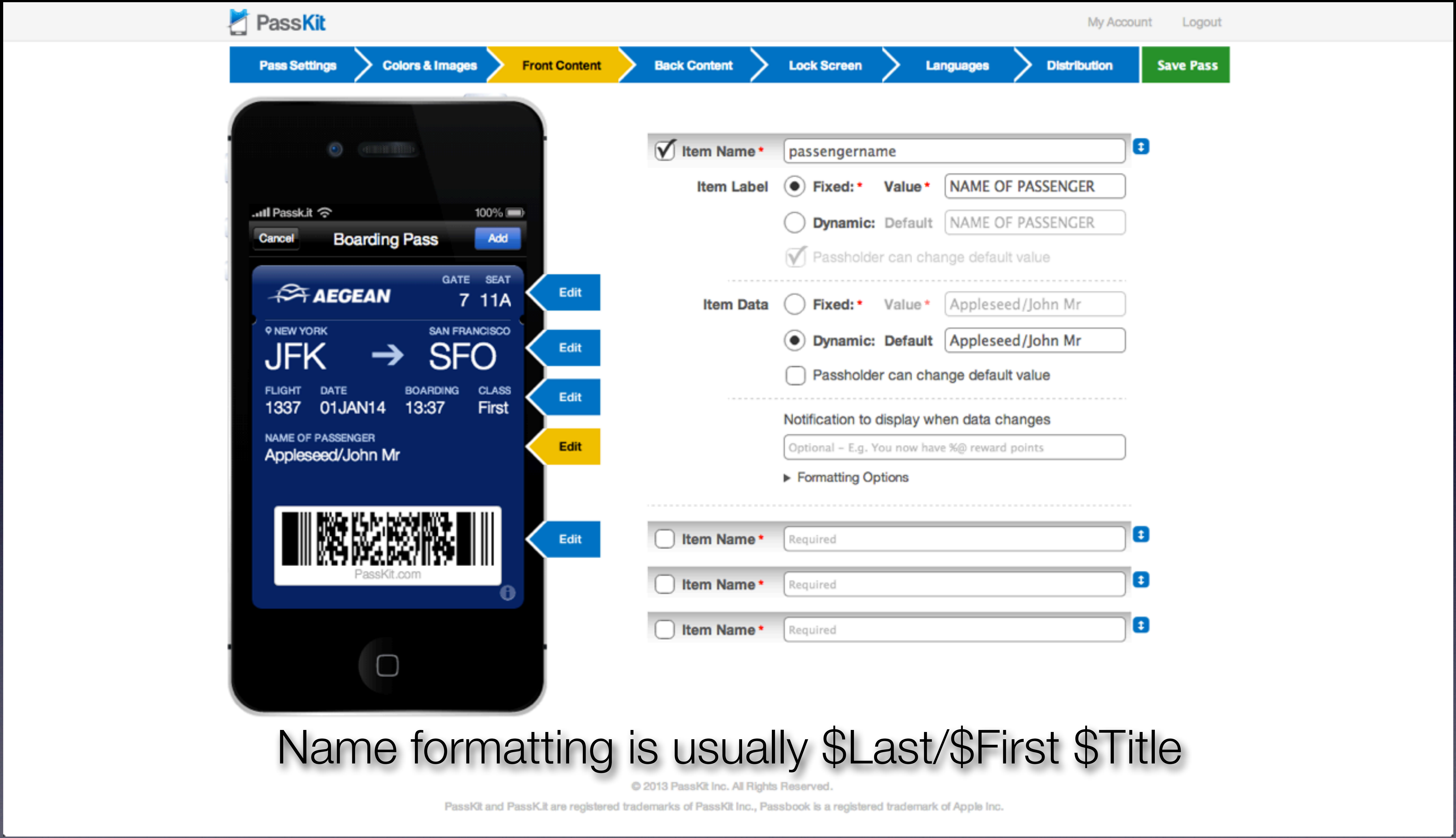
▶ Formatting Options

☑ Item Name*: flyto

© 2013 PassKit Inc. All Rights Reserved.

PassKit and PassK.it are registered trademarks of PassKit Inc., Passbook is a registered trademark of Apple Inc.

© AEGEAN AIRLINES S.A. - Use under Directive 2001/29/EC



AEGEAN

GATE 7 SEAT 11A

NEW YORK JFK → SAN FRANCISCO SFO

FLIGHT	DATE	BOARDING	CLASS
1337	01JAN14	13:37	First

NAME OF PASSENGER
Appleseed/John Mr

☑ Item Name* passengername

Item Label ● Fixed:* Value* NAME OF PASSENGER
○ Dynamic: Default NAME OF PASSENGER
☑ Passholder can change default value

Item Data ○ Fixed:* Value* Appleseed/John Mr
● Dynamic: Default Appleseed/John Mr
□ Passholder can change default value

Notification to display when data changes
Optional – E.g. You now have %@ reward points

▸ Formatting Options

□ Item Name* Required

□ Item Name* Required

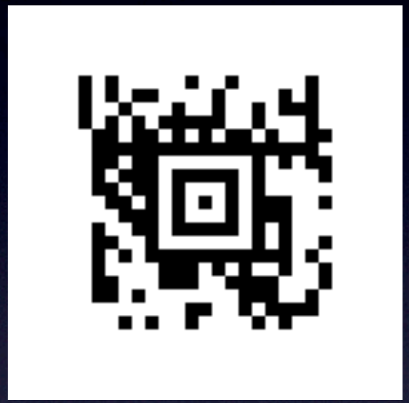
□ Item Name* Required

Name formatting is usually $Last/$First $Title

The Bar Code

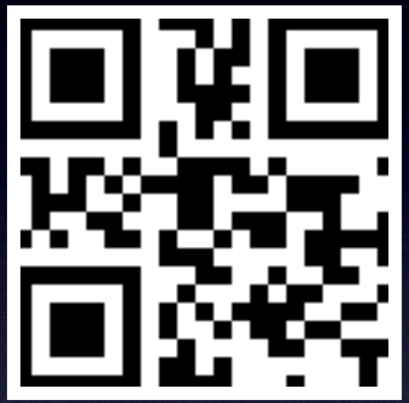
(And how to defeat it)

Types of bar codes



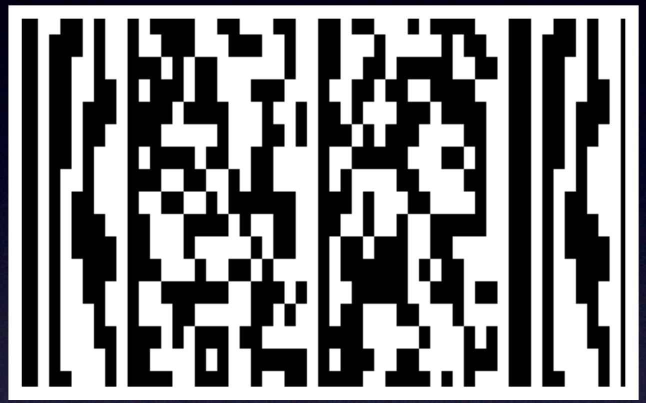
Aztec Code

Most common barcode. Has one alignment tile in the middle.



QR Code

It has three alignment tiles in three of the corners.



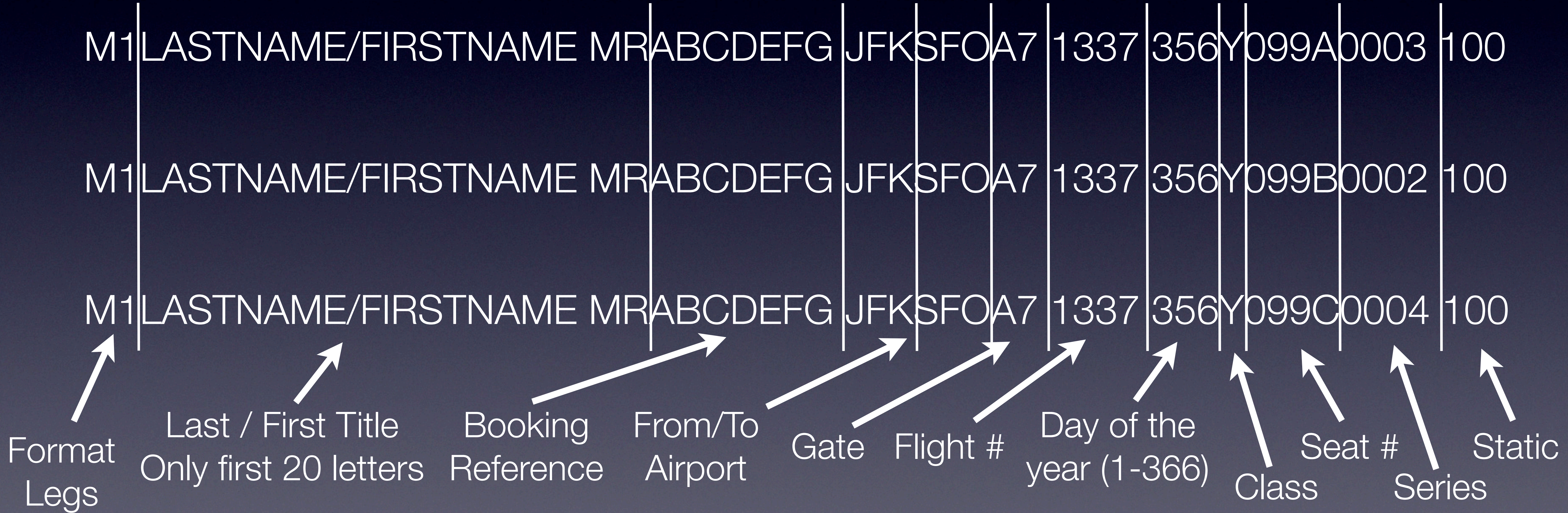
PDF417

Horizontal alignment. Resembles the traditional product barcodes.

Decoding the bar code

All smartphones can read these codes in our days. You can download a free app and decode them. At this point you need a few valid passes to compare the plaintext.

Decoded Aztec Codes



```
M1LASTNAME/FIRSTNAME MRABCDEFG JFKSFOA7 1337 356Y099A0003 100

M1LASTNAME/FIRSTNAME MRABCDEFG JFKSFOA7 1337 356Y099B0002 100

M1LASTNAME/FIRSTNAME MRABCDEFG JFKSFOA7 1337 356Y099C0004 100
```

Format
Legs

Last / First Title
Only first 20 letters

Booking
Reference

From/To
Airport

Gate

Flight #

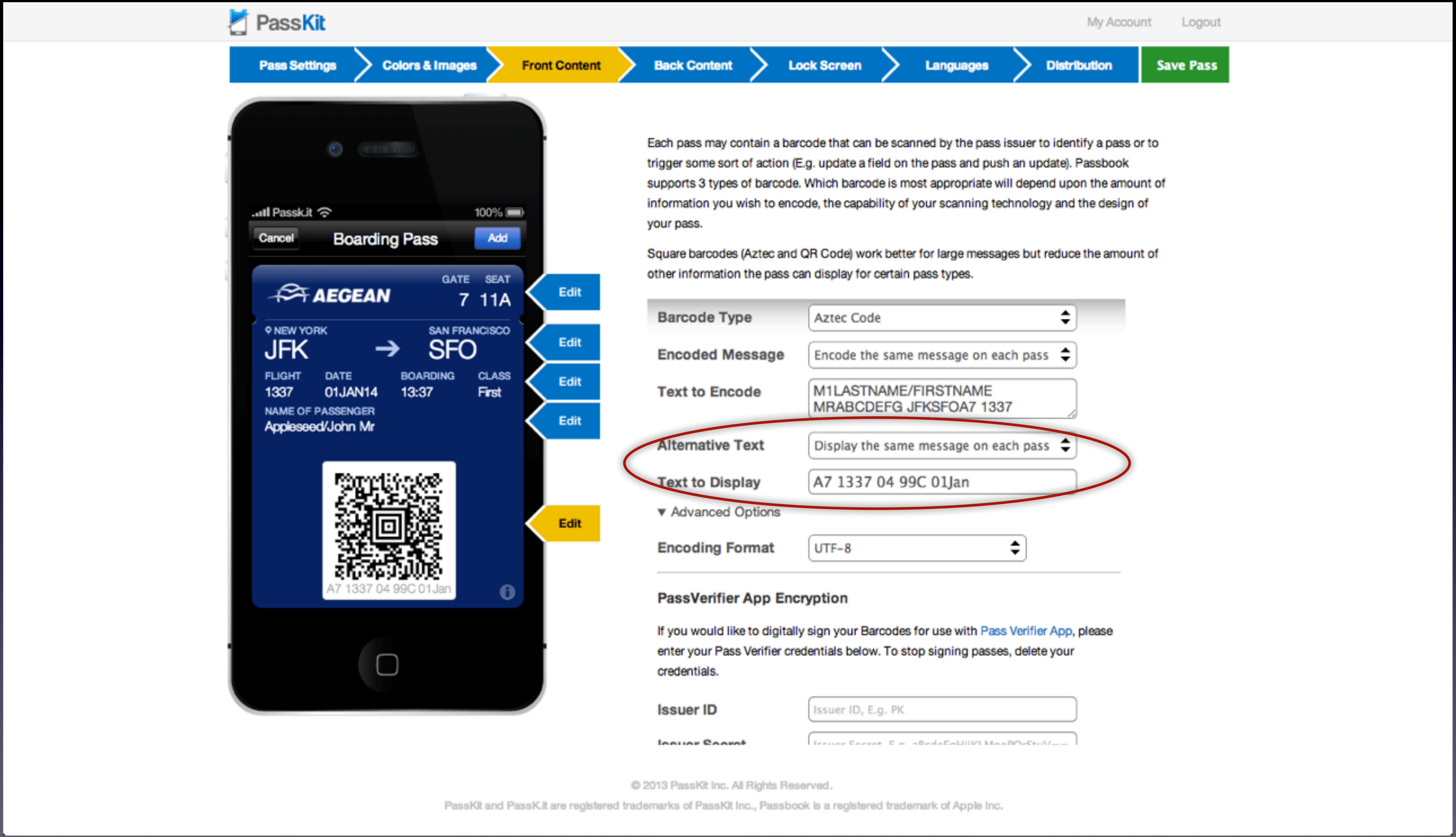
Day of the
year (1-366)

Class

Seat #

Series

Static



Each pass may contain a barcode that can be scanned by the pass issuer to identify a pass or to trigger some sort of action (E.g. update a field on the pass and push an update). Passbook supports 3 types of barcode. Which barcode is most appropriate will depend upon the amount of information you wish to encode, the capability of your scanning technology and the design of your pass.

Square barcodes (Aztec and QR Code) work better for large messages but reduce the amount of other information the pass can display for certain pass types.

Barcode Type	Aztec Code
Encoded Message	Encode the same message on each pass
Text to Encode	M1LASTNAME/FIRSTNAME MRABCDEFG JFKSFOA7 1337
Alternative Text	Display the same message on each pass
Text to Display	A7 1337 04 99C 01Jan

▾ Advanced Options

Encoding Format	UTF-8

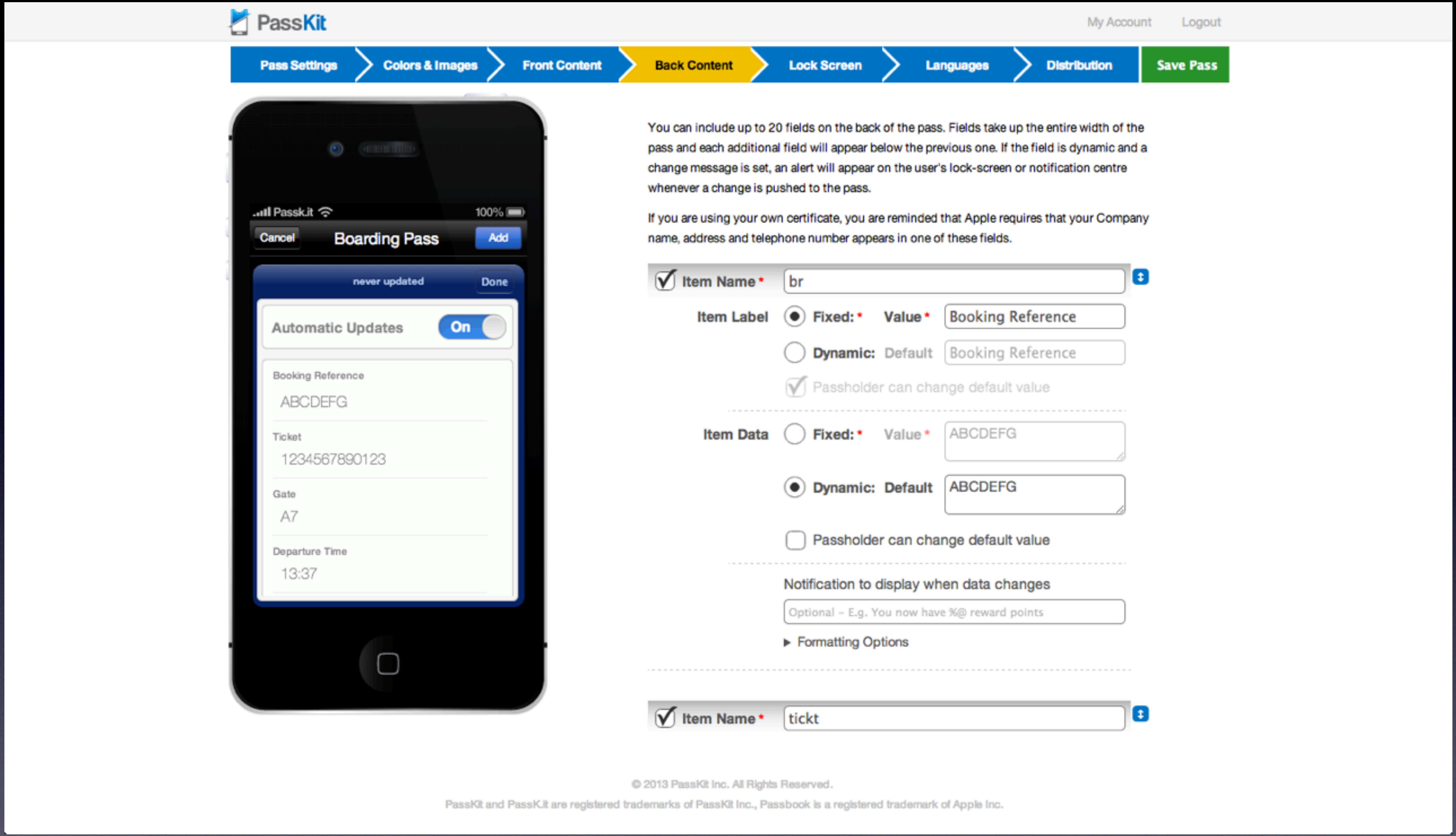
PassVerifier App Encryption

If you would like to digitally sign your Barcodes for use with Pass Verifier App, please enter your Pass Verifier credentials below. To stop signing passes, delete your credentials.

Issuer ID	Issuer ID, E.g. PK
Issuer Secret	

© 2013 PassKit Inc. All Rights Reserved.

PassKit and PassK.it are registered trademarks of PassKit Inc., Passbook is a registered trademark of Apple Inc.



Automatic Updates On

Booking Reference
ABCDEFG

Ticket
1234567890123

Gate
A7

Departure Time
13:37

You can include up to 20 fields on the back of the pass. Fields take up the entire width of the pass and each additional field will appear below the previous one. If the field is dynamic and a change message is set, an alert will appear on the user's lock-screen or notification centre whenever a change is pushed to the pass.

If you are using your own certificate, you are reminded that Apple requires that your Company name, address and telephone number appears in one of these fields.

☑ Item Name* br

Item Label ● Fixed:* Value* Booking Reference
○ Dynamic: Default Booking Reference
☑ Passholder can change default value

Item Data ○ Fixed:* Value* ABCDEFG
● Dynamic: Default ABCDEFG
□ Passholder can change default value

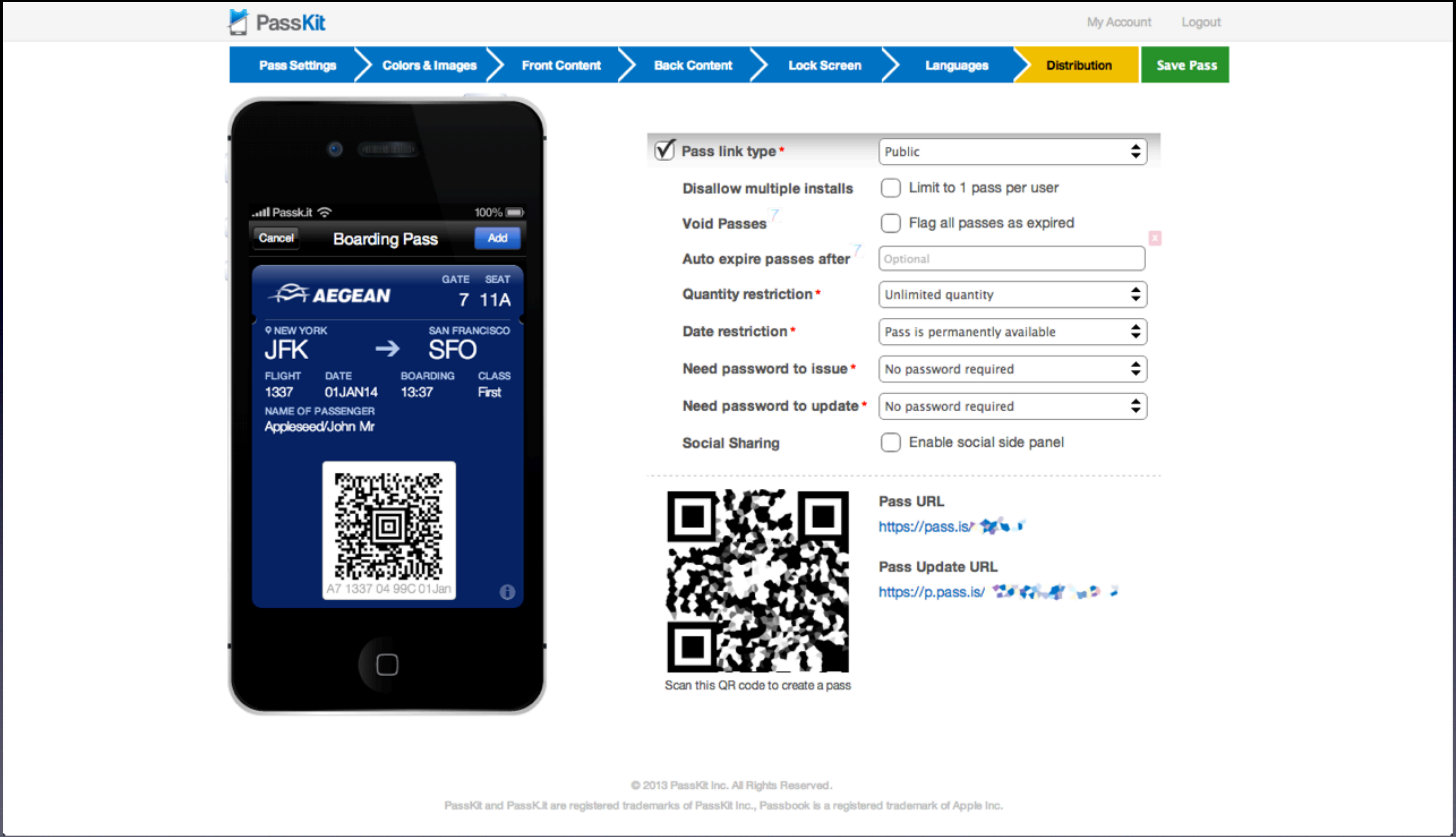
Notification to display when data changes
Optional – E.g. You now have %@ reward points

▸ Formatting Options

☑ Item Name* tickt

© 2013 PassKit Inc. All Rights Reserved.
PassKit and PassK.it are registered trademarks of PassKit Inc., Passbook is a registered trademark of Apple Inc.

Extremely difficult to find pictures of the back side.
Extremely rare to be checked by anyone though.



.ııl Passk.it 100%

Cancel Boarding Pass Add

AEGEAN

GATE 7 SEAT 11A

NEW YORK JFK → SAN FRANCISCO SFO

FLIGHT 1337 DATE 01JAN14 BOARDING 13:37 CLASS First

NAME OF PASSENGER Appleseed/John Mr

A7 1337 04 99C 01Jan

☑ Pass link type * Public

Disallow multiple installs □ Limit to 1 pass per user

Void Passes □ Flag all passes as expired

Auto expire passes after Optional

Quantity restriction * Unlimited quantity

Date restriction * Pass is permanently available

Need password to issue * No password required

Need password to update * No password required

Social Sharing □ Enable social side panel

Pass URL

https://pass.is/[redacted]

Pass Update URL

https://p.pass.is/[redacted]

Scan this QR code to create a pass

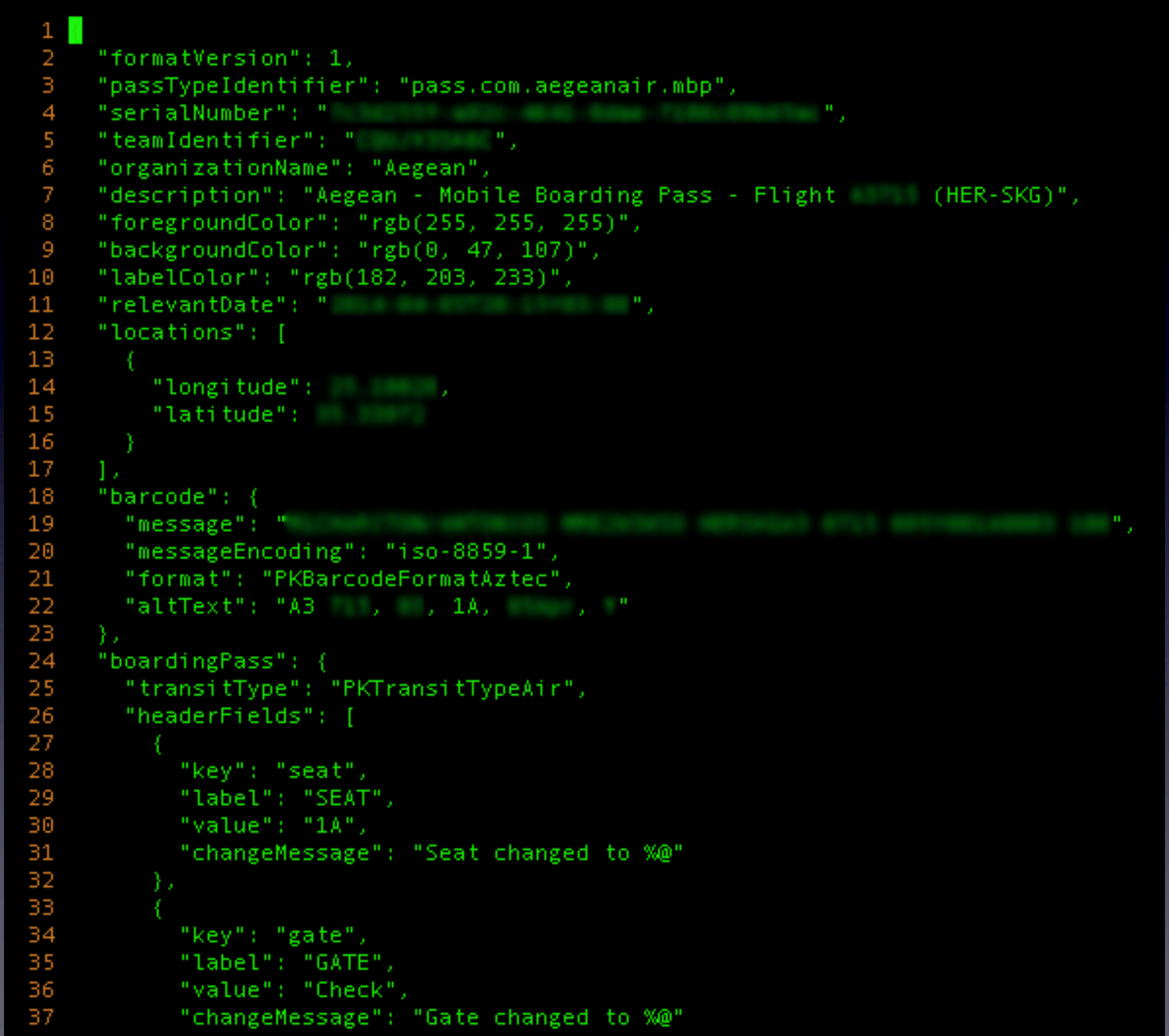
© 2013 PassKit Inc. All Rights Reserved.

PassKit and PassK.it are registered trademarks of PassKit Inc., Passbook is a registered trademark of Apple Inc.

© AEGEAN AIRLINES S.A. - Use under Directive 2001/29/EC

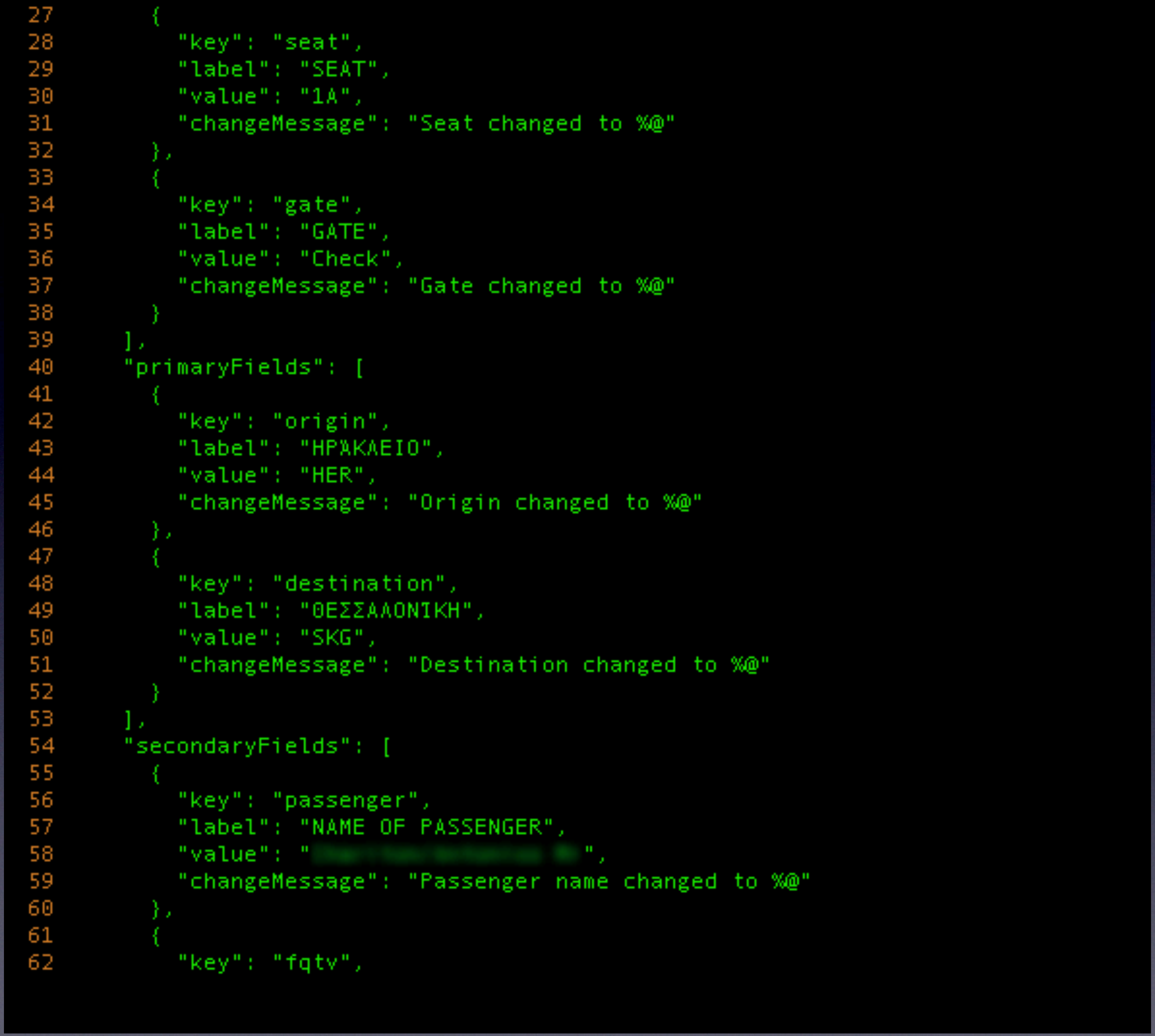
I’m a Developer!

Good for you!



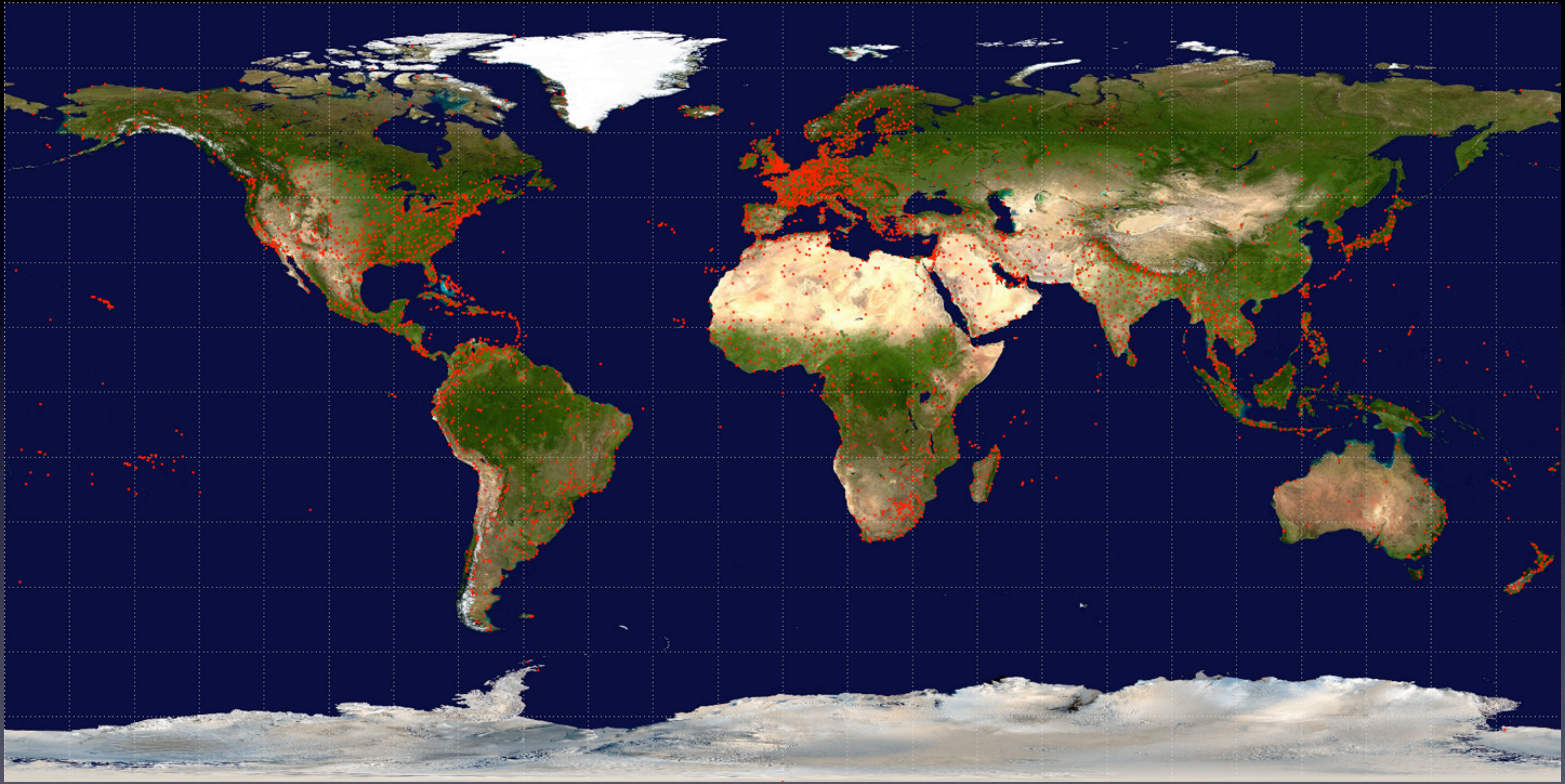
```

  "formatVersion": 1,
  "passTypeIdentifier": "pass.com.aegeanair.mbp",
  "serialNumber": "[redacted]",
  "teamIdentifier": "[redacted]",
  "organizationName": "Aegean",
  "description": "Aegean - Mobile Boarding Pass - Flight [redacted] (HER-SKG)",
  "foregroundColor": "rgb(255, 255, 255)",
  "backgroundColor": "rgb(0, 47, 107)",
  "labelColor": "rgb(182, 203, 233)",
  "relevantDate": "[redacted]",
  "locations": [
    {
      "longitude": [redacted],
      "latitude": [redacted]
    }
  ],
  "barcode": {
    "message": "[redacted]",
    "messageEncoding": "iso-8859-1",
    "format": "PKBarcodeFormatAztec",
    "altText": "A3 [redacted], [redacted], 1A, [redacted], [redacted]"
  },
  "boardingPass": {
    "transitType": "PKTransitTypeAir",
    "headerFields": [
      {
        "key": "seat",
        "label": "SEAT",
        "value": "1A",
        "changeMessage": "Seat changed to %@"
      },
      {
        "key": "gate",
        "label": "GATE",
        "value": "Check",
        "changeMessage": "Gate changed to %@"
```



```
      {
        "key": "seat",
        "label": "SEAT",
        "value": "1A",
        "changeMessage": "Seat changed to %@"
      },
      {
        "key": "gate",
        "label": "GATE",
        "value": "Check",
        "changeMessage": "Gate changed to %@"
      }
    ],
    "primaryFields": [
      {
        "key": "origin",
        "label": "ΗΡΑΚΛΕΙΟ",
        "value": "HER",
        "changeMessage": "Origin changed to %@"
      },
      {
        "key": "destination",
        "label": "ΘΕΣΣΑΛΟΝΙΚΗ",
        "value": "SKG",
        "changeMessage": "Destination changed to %@"
      }
    ],
    "secondaryFields": [
      {
        "key": "passenger",
        "label": "NAME OF PASSENGER",
        "value": "[redacted]",
        "changeMessage": "Passenger name changed to %@"
      },
      {
        "key": "fqtv",
```

I have the Pass. Now what?



© AEGEAN AIRLINES S.A. - Use under Directive 2001/29/EC

All Gates
Security Check Point
Please
Wait
Here

Terminal Cornucopia

Evan Booth

#HITB2013AMS

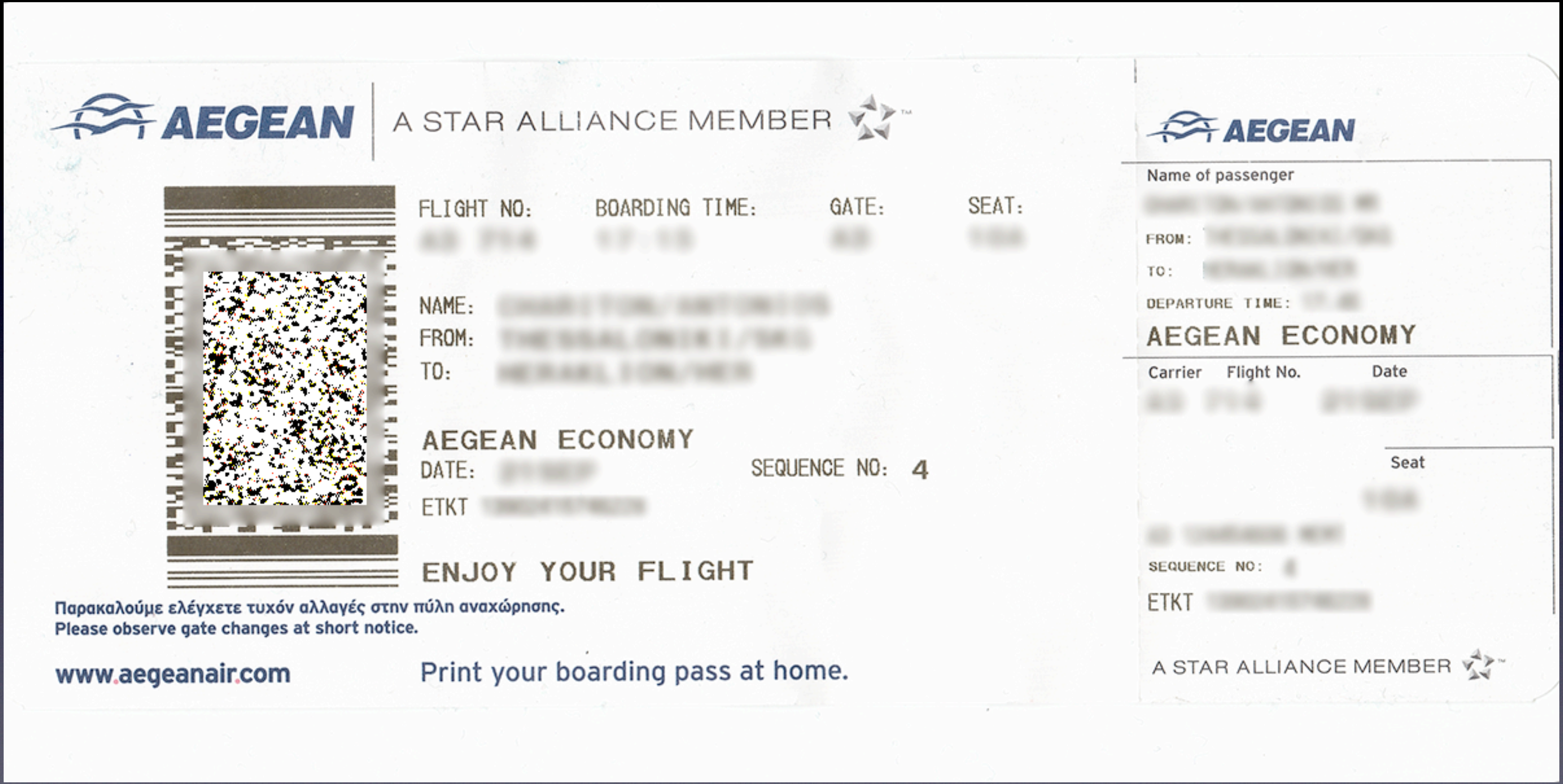
DO NOT ATTEMPT ANY OF THESE!

19:17
88
19:17

Αναχωρήσεις / Departures
Αναχωρήσεις / Departures
Αναχωρήσεις / Departures
Καλό ταξίδι
eticket
AEGEAN
ATHENS
4
123
122
121
120
AEGEAN
eticket
AEGEAN

on the gallery of Departure
257
256
STAR ALLIANCE
raport

A World Best Air Hub
Self Check-in
IIAC



AEGEAN | A STAR ALLIANCE MEMBER

FLIGHT NO: [redacted]
BOARDING TIME: [redacted]
GATE: [redacted]
SEAT: [redacted]

NAME: [redacted]
FROM: [redacted]
TO: [redacted]

AEGEAN ECONOMY
DATE: [redacted]
SEQUENCE NO: 4
ETKT [redacted]

ENJOY YOUR FLIGHT

Παρακαλούμε ελέγχετε τυχόν αλλαγές στην πύλη αναχώρησης.
Please observe gate changes at short notice.

www.aeganair.com

Print your boarding pass at home.

AEGEAN

Name of passenger
[redacted]
FROM: [redacted]
TO: [redacted]
DEPARTURE TIME: [redacted]
AEGEAN ECONOMY

Carrier	Flight No.	Date
[redacted]	[redacted]	[redacted]

Seat
[redacted]

[redacted]
SEQUENCE NO: [redacted]
ETKT [redacted]

A STAR ALLIANCE MEMBER

All Gates
Security Check Point
B2
HERSHEY'S
Please
Wait
Here

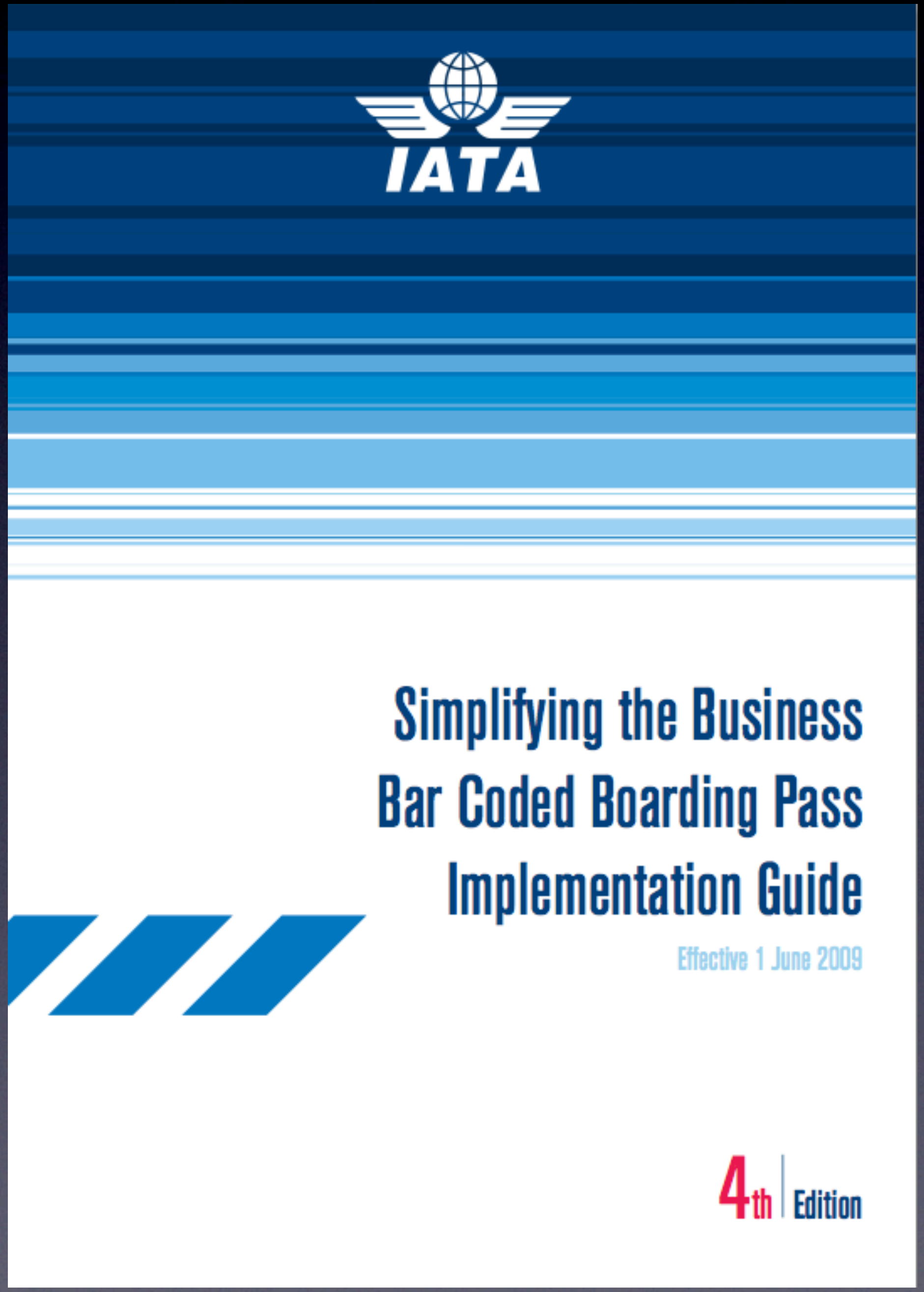
88
19:17

Enjoy your trip!

Bonus

A World Best Air Hub
Self Check-in
IIAC

Citations



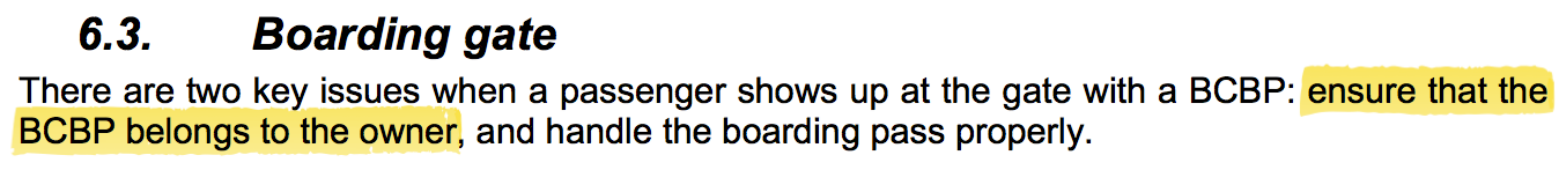
IATA

Simplifying the Business

Bar Coded Boarding Pass Implementation Guide

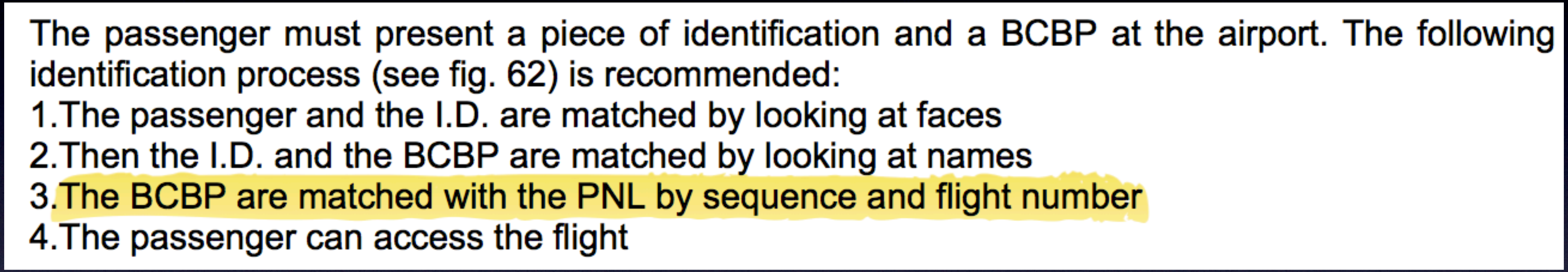
Effective 1 June 2009

4th Edition



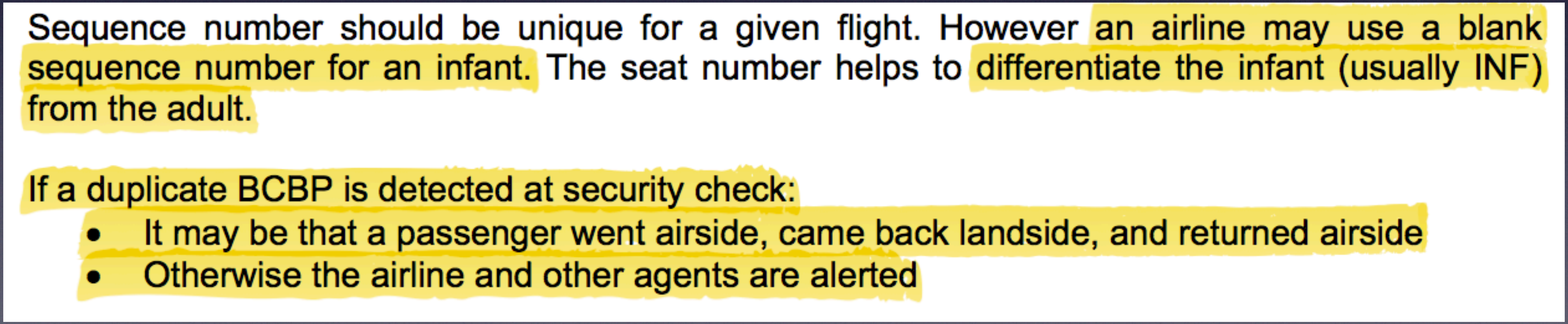
6.3. Boarding gate

There are two key issues when a passenger shows up at the gate with a BCBP: ensure that the BCBP belongs to the owner, and handle the boarding pass properly.



The passenger must present a piece of identification and a BCBP at the airport. The following identification process (see fig. 62) is recommended:

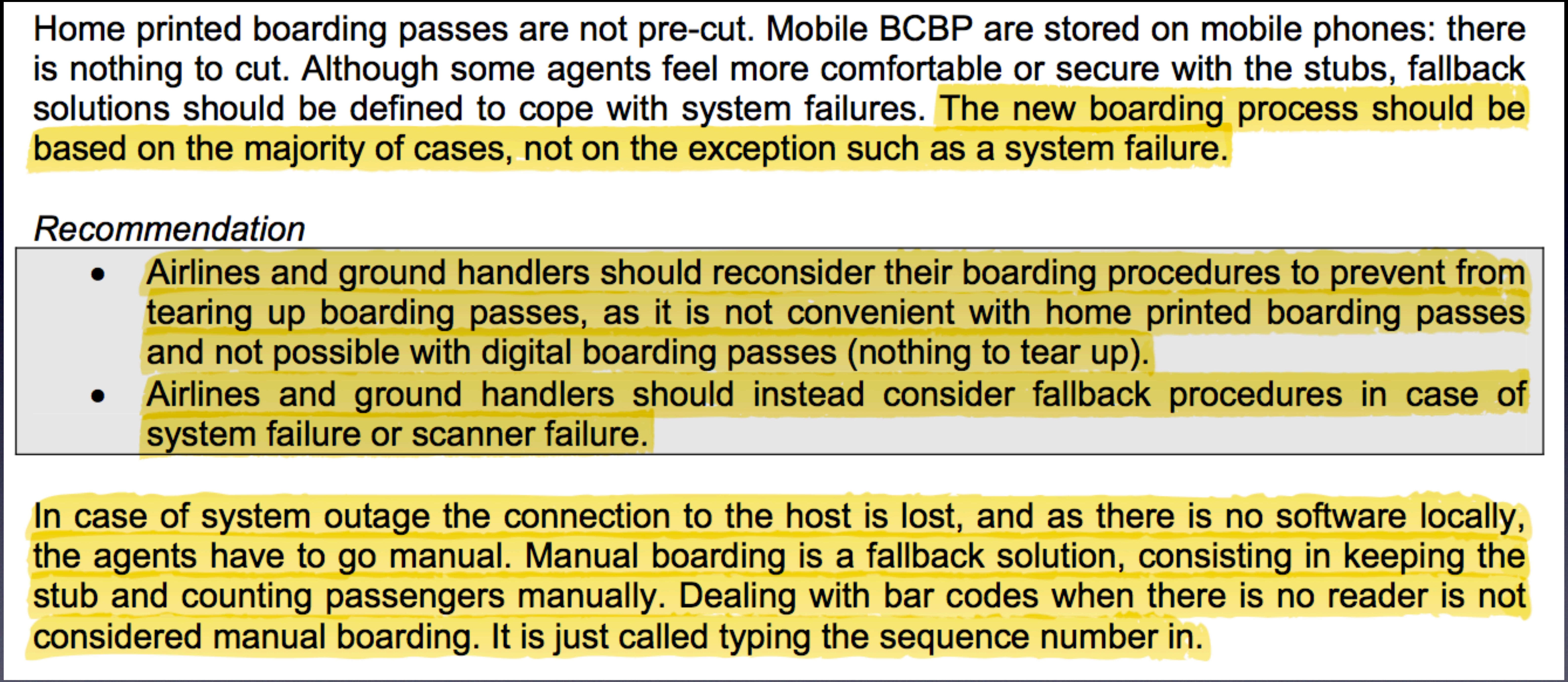
1.The passenger and the I.D. are matched by looking at faces
2.Then the I.D. and the BCBP are matched by looking at names
3.The BCBP are matched with the PNL by sequence and flight number
4.The passenger can access the flight



Sequence number should be unique for a given flight. However an airline may use a blank sequence number for an infant. The seat number helps to differentiate the infant (usually INF) from the adult.

If a duplicate BCBP is detected at security check:

- It may be that a passenger went airside, came back landside, and returned airside
- Otherwise the airline and other agents are alerted

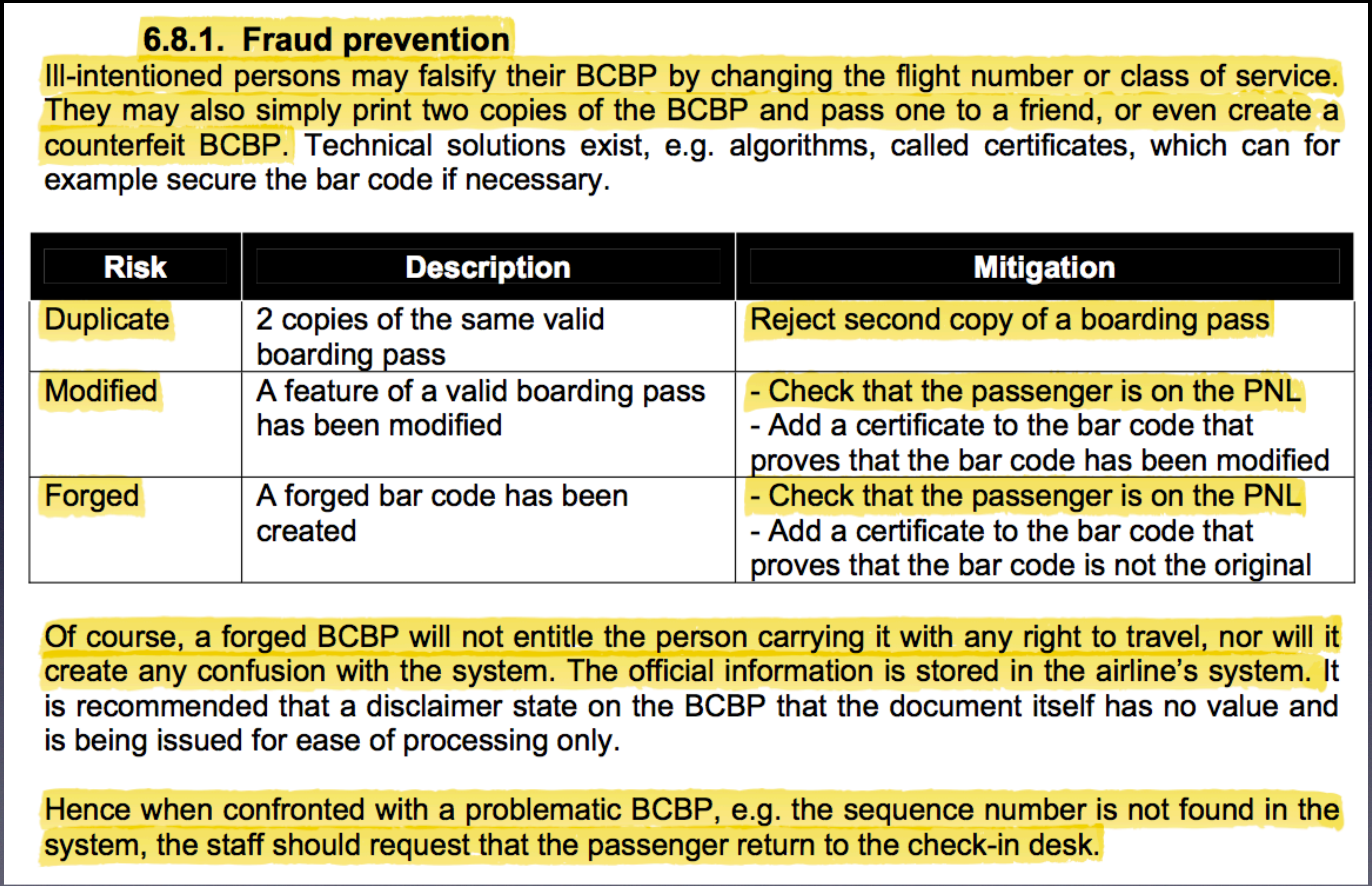


Home printed boarding passes are not pre-cut. Mobile BCBP are stored on mobile phones: there is nothing to cut. Although some agents feel more comfortable or secure with the stubs, fallback solutions should be defined to cope with system failures. The new boarding process should be based on the majority of cases, not on the exception such as a system failure.

Recommendation

- Airlines and ground handlers should reconsider their boarding procedures to prevent from tearing up boarding passes, as it is not convenient with home printed boarding passes and not possible with digital boarding passes (nothing to tear up).
- Airlines and ground handlers should instead consider fallback procedures in case of system failure or scanner failure.

In case of system outage the connection to the host is lost, and as there is no software locally, the agents have to go manual. Manual boarding is a fallback solution, consisting in keeping the stub and counting passengers manually. Dealing with bar codes when there is no reader is not considered manual boarding. It is just called typing the sequence number in.



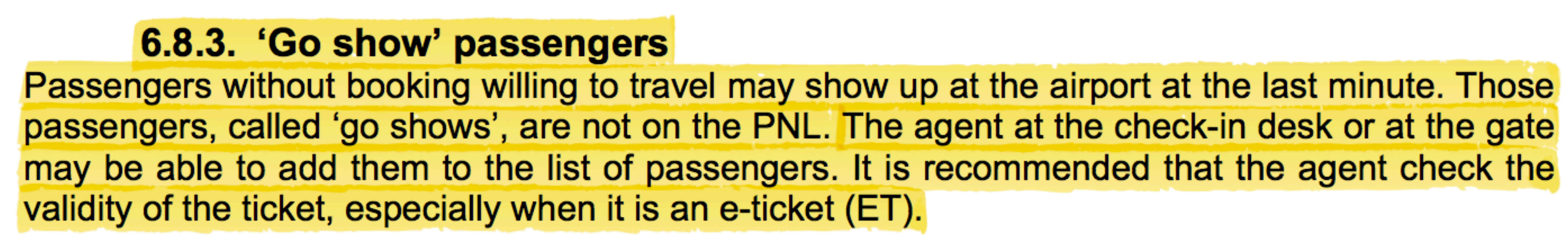
6.8.1. Fraud prevention

Ill-intentioned persons may falsify their BCBP by changing the flight number or class of service. They may also simply print two copies of the BCBP and pass one to a friend, or even create a counterfeit BCBP. Technical solutions exist, e.g. algorithms, called certificates, which can for example secure the bar code if necessary.

Risk	Description	Mitigation
Duplicate	2 copies of the same valid boarding pass	Reject second copy of a boarding pass
Modified	A feature of a valid boarding pass has been modified	- Check that the passenger is on the PNL - Add a certificate to the bar code that proves that the bar code has been modified
Forged	A forged bar code has been created	- Check that the passenger is on the PNL - Add a certificate to the bar code that proves that the bar code is not the original

Of course, a forged BCBP will not entitle the person carrying it with any right to travel, nor will it create any confusion with the system. The official information is stored in the airline's system. It is recommended that a disclaimer state on the BCBP that the document itself has no value and is being issued for ease of processing only.

Hence when confronted with a problematic BCBP, e.g. the sequence number is not found in the system, the staff should request that the passenger return to the check-in desk.



6.8.3. ‘Go show’ passengers

Passengers without booking willing to travel may show up at the airport at the last minute. Those passengers, called ‘go shows’, are not on the PNL. The agent at the check-in desk or at the gate may be able to add them to the list of passengers. It is recommended that the agent check the validity of the ticket, especially when it is an e-ticket (ET).

Thank you

Any questions?