BEST PRACTICES:
BEACON LOCATION SECURITY
AND ENCRYPTION

JAMES BUCHHEIM, CEO
BEACONS OVERVIEW

- Beacons interact with standard mobile devices and applications
- Simple, inexpensive, small and long-life battery-powered
- Key advantage: Contextual engagement at right place, right time
BEACONS TRENDS

• Apple iBeacon Hype: iBeacon is just a Protocol

• Google standardized BLE

• IoT with unlimited contextual apps and discovery services

• Beacon Cloud-based ecosystem a MUST for management

• Privacy and Security Challenges – Extreme care and security to ensure beacons respect Privacy (based on a GSMA study)
THE OPPORTUNITY

**B2B**
- In Transit
- In storage
- Manufacture
- Public Area

**B2C**
- On Entry
- In aisle/department
- At POS
- In transit

**WHERE**

**WHAT**
- Track an app
- Track a device
- Track a person
- Track an item

- Deliver content
- Make payments
- Reminder
- Check-in
VERTICAL OPPORTUNITY

B2C SECTORS

Doctors Surgery
Hospital
Pharmacy
Healthcare

Shops
Malls
Retail

Events
Theatre / Cinema
Stadium

Train
Airport
Road
Transport

Other Public
Outdoor Media
Advertising

Bars
Restaurants
Hotels
Hospitality
• When? Care should be taken when deploying beacons to ensure their infrastructure cannot be used by unauthorized third parties

• Where? In any third party apps or customer identifiable data collection

• How?
  - Use a non-deployer unique UUID
  - Ensure Major And Minor schema is not decodable by 3rd parties (random)
  - Change major and minor frequently (example: once per minute)
  - Deploy and configure with a secure, private password
Four Best Practice findings identified:

1. Always offer customer value in return for knowing their location
2. Ensure customers fully understand how their location data used/recorded
3. Take steps to protect live or historical data in mobile app or other platform
4. Do not share user location data with 3rd parties without permission(s)
UUID
- Used in beacon settings to identify the owner/deployer

MAJOR/MINOR
- Major identifies location
  Minor Identifies micro-location within a location

PROTECTION SCHEMES

UUID: B9407F30-6A19-4B2D-8556B57FE6D
UUID: A7408V30-63E-A8U1-25556B57A96R
UUID: F8AD3E82-0D91-4D9B-B5C7-732474426

Single
UUID: F8AD3E82-0D91-4D9B-B5C7-732474426

Retailer A
UUID: B9407F30-6A19-4B2D-8556B57FE6D
Retailer B
UUID: A7408V30-63E-A8U1-25556B57A96R

UUID: F8AD3E82-0D91-4D9B-B5C7-732474426
ENCRYPTION

• Data encryption protection can be implemented on beacon or cloud services

• Apps that carry trigger value transactions should utilize encrypted beacons

• Sellers and deployers of beacons should provide guidance on why and how to utilize beacon technology in a responsible and secure manner and consider the benefits of adding encryption
Three Basic Security/Encryption Models:

1. **STANDARD:** App holds all beacon estate data locally

2. **CLOUD:** App queries a cloud-based platform with UUID, Major and Minor for location data returned

3. **CLOUD SECURE:** Beacon data is fully encrypted and only decrypted by cloud platform, which returns to the app detailed location data
NEXT STEP
Beacons Security/Privacy

• Meet StickNFind in exhibit area to learn more on managing cloud security with our new BluZone beacon cloud-based beacon control dashboard

• Email @ jimmy@sticknfind.com