Cybersecurity and the Role of Mobile Financial Transactions

Jackie McCarthy
Director, Regulatory Affairs
NCSL Capitol Forum
December 5, 2016

Outline

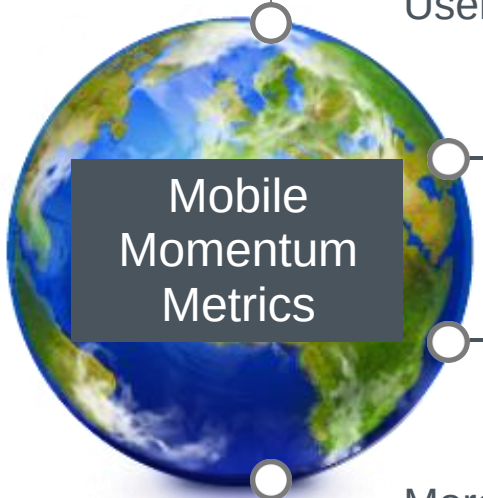
- About CTIA and wireless's role in payments
- Mobile Payments – Types and Trends
- Key Players
- Regulatory Issues & Initiatives
- Focus on Authentication
- Mobile Cyber Tips and Lessons Learned

About CTIA

- Non-profit membership association representing the wireless industry (carriers, device makers, vendors and app developers)
- Advocates at all levels of government
- Coordinates industry initiatives & outreach to brands and entrepreneurs in the retail/payments/banking sector through our Mobile Financial Services and Cybersecurity Working Groups

Global Mobile Data Traffic Drivers

By 2019:



More Mobile Users

2014	2019
4.3 Billion	5.2 Billion

More Mobile Connections

2014	2019
7.4 Billion	11.5 Billion

Faster Mobile Speeds

2014	2019
1.7 Mbps	4.0 Mbps

More Mobile Video

2014	2019
55% of Traffic	72% of Traffic

Source: Cisco VNI Global Mobile Data Traffic Forecast, 2014–2019

Types of Mobile Payments

- Mobile Wallets (payment info communicated via secure near-field communications)
  - Apple
  - Google
  - Samsung
  - Card Networks like MasterCard
- Mobile Acceptance (Square)
- Retailer or Bank App (Starbucks)
- Mobile Web Browser
- Peer-to-Peer Transfers (Venmo)

Mobile Payments Market Data & Observations

- 2011: Google Wallet; 2014: Apple Pay, Samsung Pay
- US in-store mobile payment volume will reach $75B in 2016, with 80% compound annual growth rate until 2020 (estimated $503B volume)(Business Insider)
- 39% of all US mobile users made a mobile payment in 2015 (Federal Reserve Bank)
- Market fragmentation and consumer acceptance are barriers, but growth continues
- Loyalty and affinity programs spark consumer adoption

Key Wireless Players in Mobile Payments

- Carriers: Provide robust wireless broadband coverage and network security services.
- Device Makers: Manufacture smartphones and other wireless devices (like wearables) as chip, battery and radio elements evolve
- Operating Systems: Mobile software ecosystems, each with their own mobile payments features, with security features like app onboarding management, permissions management and developer outreach
- Apps: A maturing marketplace for app tools and features to process secure data (including payment info) more effectively.

Regulatory Issues & Initiatives

- July 2016: CTIA and 16 wireless companies announce **Smartphone Anti-Theft Voluntary Commitment** as part of the CTIA Consumer Code.
  - CTIA maintains a **stolen phones database** with unique IDs of phones reported lost/stolen.
  - All smartphones will include **anti-theft tool** with capability to remotely wipe user data and render smartphone inoperable to an unauthorized user.
- The communications, financial services, retail and other sectors **share cybersecurity info** in a safe environment via NIST's Cybersecurity Framework, which encourages industry-led convening with public-sector participation (DHS, FCC, Treasury, financial services regulators).

Focus on Authentication

- NIST is considering the impact of **two-factor authentication** measures to verify user identity for consumer-facing sites like SSA and VA.
- Many of these agencies use **SMS/text messaging** for verification measures to accountholders, as SMS is widely used across consumer segments, even among non-smartphone users. According to our research, half of consumers have used mobile to validate their ID, and 87% say mobile authentication is very/somewhat easy to use.

Mobile Cybersecurity Tips & Lessons Learned

- Use good mobile "cyber hygiene" to reduce risks.
  - Update operating systems and apps promptly. Don't click on suspicious links. Use particular caution when surfing the Web on public wi-fi.
  - Download official security apps. Use a device password. Promptly alert carrier when device is lost or stolen.
  - Train staff on indicators of social engineering/fraud (spike in account activity, high numbers of failed attempted logins).
- Implement Mobile Device Management (MDM) systems for enterprise users
- Use two-factor authentication (as described earlier) to verify accountholder identity and limit risk of identity theft/fraud.


ctia
Everything™
Wireless