Anticipating, Understanding and Preparing for New Rules for a New Mobile World

RAMP Advanced Commerce and Mobile Retail Services Summit

April 4, 2012

Andrew Lorentz
James Mann
Randy Gainer
Ronnie London

Davis Wright Tremaine LLP

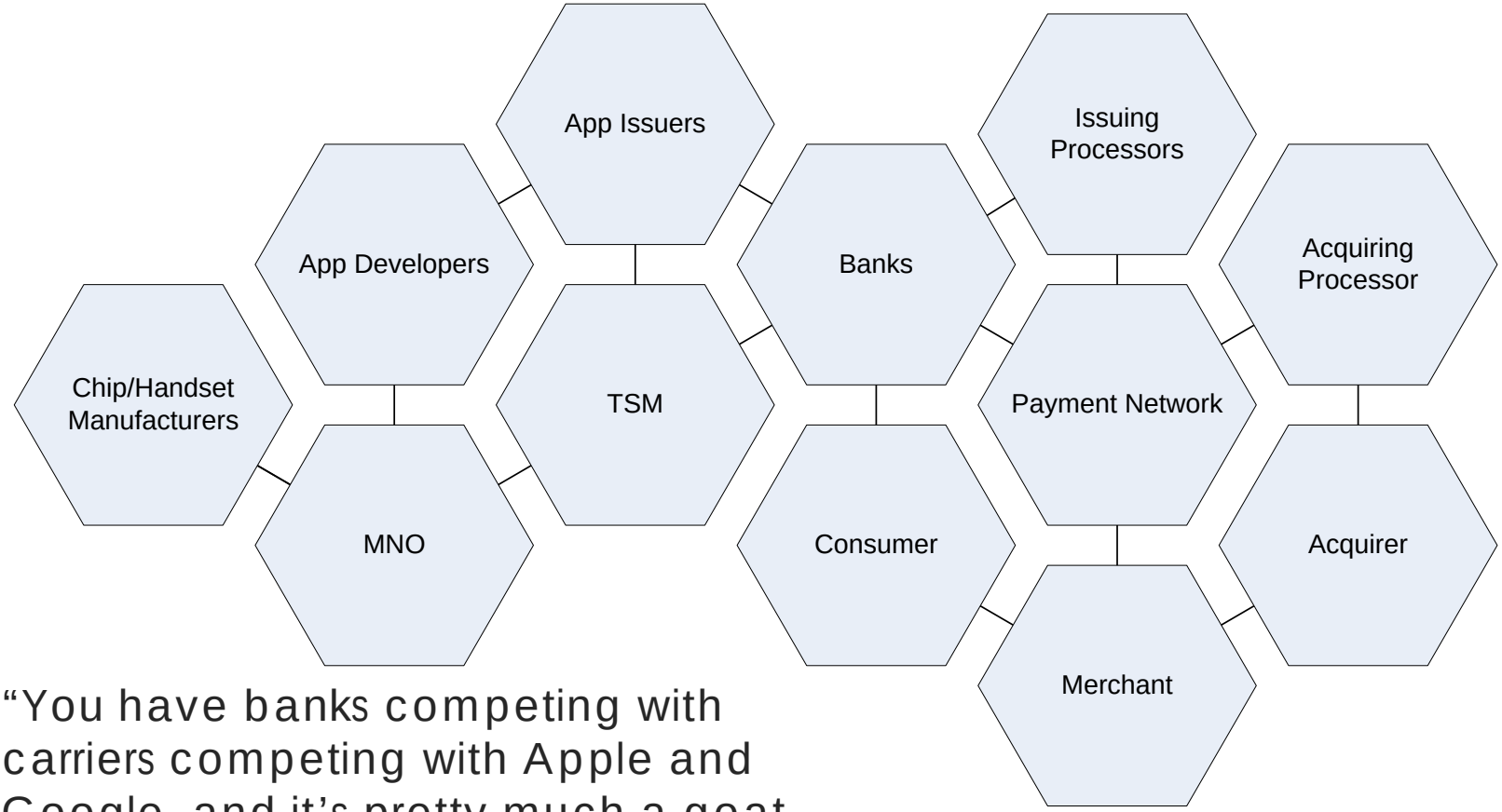
DEFINING SUCCESS TOGETHER

Contents

- Overview of mobile payments ecosystem
- Financial privacy requirements
- Data security and PCI compliance
- Mobile communications regulation

Overview of Mobile Payments Ecosystem

Players in the mobile ecosystem



"You have banks competing with carriers competing with Apple and Google, and it's pretty much a goat rodeo until someone sorts it out." Drew Sievers, chief executive of mFoundry.

Goat rodeo

Major deal points…

- Who contracts with whom?
- What revenue model? Greed and fear, but mostly fear(?)
- Who controls customer? Parallel customer relationships?
- Who is providing services to whom (if anyone…)
- Start-up costs: who pays to motivate adoption?

NOW, NEGOTIATE when there is no common language among participants: must translate among technology, banking, mobile network operators, and retailer players

Major regulatory issue (I)- who regulates?

- Existing banking regulators may predominate (Federal Reserve, FDIC, OCC, NCUA)
- State financial services regulators (and maybe Attorneys General)
- FCC for billing and consumer protection
- State public utility commissions(?)
- New CFPB for consumer protection, backed up by FTC

Major regulatory issue (II) – what laws apply?

It depends...

Bank or money transmitter-issued instruments approach ---- consumer financial services law

- Electronic Fund Transfer Act/Regulation E
- Truth in Lending Act/Equal Credit Opportunity Act/Regulations Z and B
- State Money Services Acts
- Other laws and rules: Bank Secrecy Act, Bank Service Company Act, payment network rules, (privacy, security, and marketing to come)

Carrier approach --- Cramming, Truth in Billing

Financial Privacy Requirements

Financial Privacy Requirements

- The landscape:
  - GLBA
  - FCRA
  - Other :
    - State laws (e.g., SB1)
    - Canadian/EU law

Financial Privacy Requirements

- Bottom line: restrictions on financial institutions' sharing data, especially for marketing purposes

- Problematic:
  - for development of interest profiles/graphs
  - for development of relevant real-time offers
  - for mitigation of chargeback risk

Financial Privacy Requirements

- Traditional responses – examples:
  - Non-sharing workarounds
    - problem of data-leakage
  - Third-party workarounds
  - Non opt-out populations
  - Opt-in/transaction or experience data

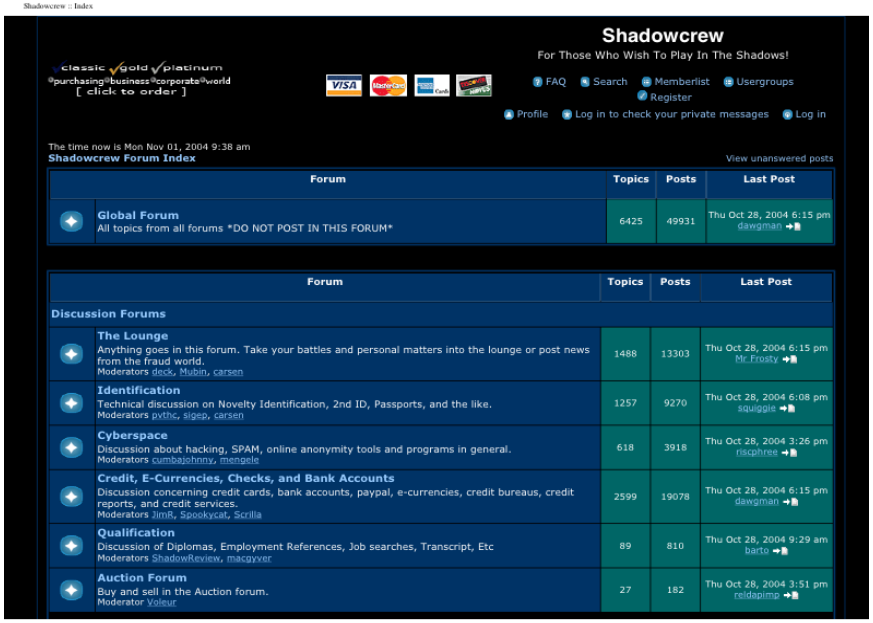
Financial Privacy Requirements

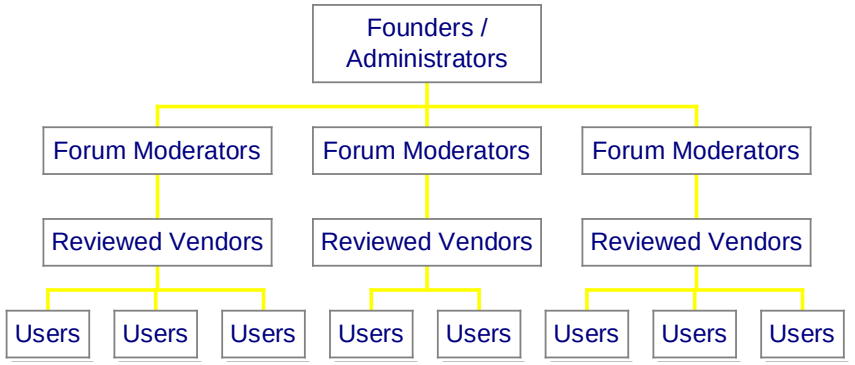
- The emerging playbook – examples:
  - Corporate transactions
  - Leveraging big data
    - Disintermediating consumer reporting agencies
    - Data-integrity issues

Data Security and PCI Compliance

Data Security and PCI Compliance

- Card data is stolen and sold by international criminal organizations
- Shadowcrew.com – one of the largest online centers for trafficking in stolen credit and bank card numbers and identity information
- 2004 federal takedown:
  - 21 arrests in U.S.
  - 7 foreign arrests
  - 27 search warrants world-wide
- 21 convictions and prosecutions in United Kingdom, Canada, Bulgaria, and Sweden





Slide created by Jenny Durkan, U.S. Attorney, W.D. Wa. Used with permission.

Data Security and PCI Compliance

- Credit card fraud complaints increased each year 2007-2009 (FTC 2010)
- U.S. card fraud estimates:
  - $8.5 billion per year, including banks and merchants, which is .4% of $2.1 trillion U.S. card payments (Aite Group 2010)
  - $100 billion per year merchants, $11 billion banks, $4.8 billion consumers (LexisNexis 2009)

Data Security and PCI Compliance

- Card data is captured by attackers in PoS systems during the split second after it is read and before it is encrypted.
- Counterfeit cards are used to make fraudulent purchases.

Data Security and PCI Compliance

1. Criminals use automated computer programs to **scan the Internet for ports** on computers in the U.S. that are **used for remote access** applications.
2. The **scan produces a list of IP addresses** for computers that have **open remote-access or VPN ports**. The list typically includes some info. that suggests the computers' functions.
3. The criminals run automated programs to **determine sign-in credentials** for the open remote-access and VPN ports.
4. The criminals **select targets** from among the computers they're able to access, remotely access those computers and any networks to which they're connected, and **identify any Point of Sale systems** used to process magnetic stripe credit and debit card payments.
5. If the criminals identify card-processing PoS systems, they **install malware** in the PoS system **that captures unencrypted card data** as it is read off of cards by the card-reading device, before the data is encrypted.
6. The malware is programmed to **store card data** on the PoS system **and then export it to a server the criminals control**, often in Europe or Asia.
7. The **exported card data is later used** by the criminals **to make counterfeit cards** or is sold online to other criminals who will do that. The counterfeit cards are then **used to buy goods and services around the world**.

Data Security and PCI Compliance

- "Malware factored into about half of the 2010 caseload and nearly 80% of all data lost." (Verizon *2011 Data Breach Investigations Report*)
- "99% of all stolen data involved the use of some form of hacking and malware." (Verizon *2011 Investigative Response Caseload Review*)

Data Security and PCI Compliance

- State data breach laws require entities that own or license unencrypted computerized personal information to promptly notify individuals if a breach of the security of the computerized system compromises the security of the information.

Data Security and PCI Compliance

- Payment card contracts and the PCI DSS require merchants to notify card associations immediately of thefts or losses of payment card data.

Data Security and PCI Compliance

1. Senior management, board members, and counsel must be notified and must plan a response
2. The breach must be investigated to determine what information was obtained, lost, or disclosed, and how the breach occurred.
3. Management must determine who else should notified – customers, law enforcement, regulators, employees, others?
4. Management must determine how the notices will be sent and must manage the notice process.
5. Inquiries and lawsuits must be responded to.
6. Security flaws must be corrected, damages paid, and all mitigation efforts documented.

Data Security and PCI Compliance

- 2010 theft of 35,000 payment card datasets:

– Additional employee wages	$94,893
– Temp. staffing	$82,773
– Forensic investigation	$93,020
– PCI compliance	$22,200
– New hosting service	$185,880
– Network redesign	$17,000
– New hardware	$65,460
– New software	$27,241
– Legal	$30,000
– PCI fines	$15,000
– Customer notices, call center, credit restoration services ($6.25/customer)	$218,750
– Lost business during temporary shutdown	$159,784
– **Total**	**$1,012,001**

Data Security and PCI Compliance

- **If** cardholders incur actual damages, they may have viable negligence claims for failure to secure card data and for breach of an implied contract to do so. (*Anderson v. Hannaford Bros.*, 1st Cir. 2011)
- Card associations may impose fines of up to $500,000 per incident, plus additional monthly fines until the merchant complies with the PCI DSS.

Data Security and PCI Compliance

- Cryptograms and dynamic CVV from NFC-enabled phones can improve security.
- Cryptograms:
  - **SE includes crypto-processor** that can support a PKI key unique to each SE.
  - The crypto-processor uses the private key to generate a **cryptogram with transaction-unique data elements**, which **is sent to the terminal**.
  - **The cryptogram is verified** as being generated by that SE, i.e., the transaction is not being attempted from a device that does not include the SE.

Data Security and PCI Compliance

- Dynamic CVV:
  - The CVV for the card data on the device is changed for each transaction.
  - If a thief tries to re-use a CVV, it will be out-of-sync with the financial institution's back-end server and the transaction will be rejected.
  - After DDA was implemented for contactless cards in Europe, card-present fraud declined substantially.

Data Security and PCI Compliance

- NFC-enabled phones have additional security:
  - Separate passcodes can be used to access the device and to use card data.
  - The NFC antenna can be disabled until it's needed.
  - The SE is a Trusted Platform Module chip, which prevents automated attacks on the PKI key.

Data Security and PCI Compliance

- Several technical standards and "best practices" guidelines provide technical requirements for NFC-enabled phones, e.g.:
  - ISO/IEC 14443
  - NFC Forum Digital Protocol, Technical Specification
  - MasterCard Security Rules and Procedures
  - Smart Card Alliance, Issuer and Merchant Best Practices: Promoting Contactless Payments Usage and Acceptance
- These standards, when implemented by phone manufacturers and their partners, permit card data to be read by contactless card readers.

Data Security and PCI Compliance

- The PCI DSS includes limited requirements related to mobile payments:
  - **1.2.3** Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.
  - **2.1.1** For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.

Data Security and PCI Compliance

- The PCI DSS includes few requirements because it applies to card-processing network, not to the customer's payment device.
- The PCI DSS states:
  - **PCI DSS applies to all entities involved in payment card processing** – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data.
- The **PA-DSS** includes similar requirements in §§ **6.1 & 6.2**.

Data Security and PCI Compliance

- The Information Security regulations adopted by Massachusetts, includes similar requirements:
  - CMR 17.04: Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program … the following elements: ….
  - (3) Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.
- NFC-enabled phones can comply with the few applicable provisions of the PCI DSS, PA-DSS, Mass. regulations.

Mobile Communications Regulation

Mobile Communications Regulation

- Interacting with customers over mobile platforms is heavily regulated
  - FCC Telemarketing, Automated Dialing System, and Mobile CAN-SPAM Rules
  - FTC Telemarketing and Fair Trade Practice Regulation
  - State analogs to FCC & FTC Authority
  - Industry guidelines – MMA, CTIA, IAB
  - Wireless carrier rules

Mobile Communications Regulation

- FCC Telemarketing, Automated Dialing System, and Mobile CAN-SPAM Rules
  - Telephone Consumer Protection Act (TCPA) and FCC rules bar automated wireless calls – of any content, *i.e.*, sales **&** non-sales – absent prior express consent
    - Includes text-messaging, prerecorded/artificial voice calls, and auto/predictive-dialed live agent calls
    - For sales calls, clear and conspicuous prior written, signed consent is required
      - But even for non-sales, must record prior express consent
    - Sales calls also face full panoply of do-not-call regime
  - Courts strictly construe consent required
  - Private causes of action + FCC fines (up to $16K/call)

Mobile Communications Regulation

- FCC Telemarketing, Automated Dialing System, and Mobile CAN-SPAM Rules
  - Text-messages to phone numbers governed by TCPA
  - Special FCC CAN-SPAM rules govern "mobile service commercial messages" (MSCMs) to wireless domain email addresses (*e.g.*, subscriber@wirelesscarrier.com)
    - Applies only to "primarily commercial" emails like FTC CAN-SPAM, but **opt-in**, not opt-out
    - Must offer/honor after opt-in
    - Email addresses in FCC database of wireless domains (www.fcc.gov/cgb/policy/DomainNameDownload.html) must be scrubbed out except where individual addressee gives sender express prior authorization

Mobile Communications Regulation

- FTC Telemarketing and Fair Trade Practice, and Other Regulation
  - Telemarketing Sales Rule (TSR) mirrors TCPA rules, (but does not reach texting or auto/predictive-dialing cells)
    - And no private action – but FTC (and states) can enforce
  - General CAN-SPAM applies to "primarily commercial" emails to "regular" (*i.e.*, non-wireless domain) addresses
  - Children's Online Privacy Protection Act (COPPA)
    - Requires verifiable parental consent prior to knowingly collecting, using or disclosing personally identifiable information about children under 13
    - Exceptions for contests, one-time contact, email-only in some contexts

Mobile Communications Regulation

- FTC Telemarketing and Fair Trade Practice, and Other Regulation
  - Expects collection/use of personal data to fall within privacy policies, and enforces failure to honor promises made in them as deceptive or unfair trade practices
    - Preaches "privacy by design"
    - Offer simplified notice, choice, and consent, plus transparency, data security and deleting data no longer used
    - Just issued Final Report on Consumer Privacy
      - Includes call for mobile services to work toward improved privacy protections, including short, meaningful disclosures
  - Obama Administration Consumer Privacy Bill of Rights
    - Features individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability

Mobile Communications Regulation

- State analogs to FCC & FTC authority
  - Most states regulate telemarketing and/or use of ADADs in ways that can/may encompass wireless
  - Some states also purport to regulate commercial email
  - Preemption
    - TCPA allows more (but not less) restrictive state regulation of ***intra***state telemarketing, but FCC rules should preempt as to interstate calls (though states tend not to honor the preemption and FCC has not acted to force the issue)
    - CAN-SPAM Act preempts state laws purporting to regulate email qua email, except for those that target fraud or deception, and general state fraud/deception and computer crime laws can apply as well

Mobile Communications Regulation

- Industry guidelines
  - Mobile Marketing Association (MMA)
    - Global Code of Conduct calls for Notice, Choice & Consent, Customization & Constraint, Security & Accountability
    - Mobile Application Privacy Policy Framework provides model/starting-point for mobile app privacy policies (http://mmaglobal.com/whitepaper?filename=MMA_Mobile_Application_Privacy_Policy_15Dec2011PC_Update_FINAL.pdf)
  - CTIA - The Wireless Association:
    - Best Practices for Location Based Services seeks to ensure users receive meaningful notice about, and consent to, how location information will be used, disclosed and protected
  - Interactive Advertising Bureau Self-Regulatory Principles for Online Behavioral Advertising contemplate Education, Transparency, Consumer Control, Data Security, Notice of Material Changes, Special Handling of Sensitive Data

Mobile Communications Regulation

- Mobile Carrier Rules
  - Each carrier has its own set of rules for what is permissible, for example, for each type of campaign over its network, including, for instance, texts
  - To conduct SMS campaigns, must typically go through an aggregator that allows operation across carriers, which in turn have generally applicable rules, and rules applicable to each carrier
- Notable Litigation
  - Suits over location based services
  - Text-messaging class actions
  - Claims that apps store phonebook and other data

Mobile Communications Regulation

- Overarching practical tips
  - Consider adding a CPO, or at least assigning some CPO-like responsibilities
  - Maintain (or create) a good working relationship between legal and marketing
  - Establish system of internal reporting and checks and balances to detect and solve problems early, before they snowball
  - Monitor third-party vendors, partners and affiliates

Mobile Communications Regualtion

- Overarching practical tips
  - Track the way customer data is managed; ensure that those who opt-out get opted-out in the system
  - Make sure you know what data you will collect from consumers, and what uses you could possibly make of that data—and disclose that in your privacy policy
  - Make the disclosures easy to find and understandable
  - Beware of the "creeped out" factor. Privacy concerns typically arise where the intrusion seems akin to dystopian science-fiction

Questions?

- Andrew Lorentz, Partner, 202.973.4232
  andrewlorentz@dwt.com
- James Mann, Partner, 212.603.6482
  jamesmann@dwt.com
- Randy Gainer, Partner, 206.757.8047
  randygainer@dwt.com
- Ronnie London, Of Counsel, 202.973.4235
  ronnielondon@dwt.com

DWT payment**law**advisor

The DWT Payments Team addresses changes and continuities in the payments industry every day—leveraging our many years of industry experience and our presence on both coasts and in China. On **www.paymentlawadvisor.com**, we offer commentary on new developments that seem particularly significant, as well as resources that we believe can be helpful to others who are tasked with anticipating, understanding and addressing these developments.

Follow us on Twitter: @paymentLAWadv

Disclaimer

This presentation is a publication of Davis Wright Tremaine LLP. Our purpose in making this presentation is to inform our clients and friends of recent legal developments. It is not intended, nor should it be used, as a substitute for specific legal advice as legal counsel may only be given in response to inquiries regarding particular situations.

Attorney advertising. Prior results do not guarantee a similar outcome.