SO YOU WANT TO TAKE YOUR BUSINESS DIGITAL: LEGAL BASELINE AND CONSIDERATIONS
Customer Journey – Digital First

- So you want to take your business digital
  - Advantages
  - Identify points of pain
  - Gather the right team
  - Build vs. buy
  - What to watch for
  - Third-party vendor risk
Legal baseline enabling digital transactions

- ESIGN and UETA
  - Writing and signing
  - Consent
  - Retention
  - Smart contracts
- Case Law
  - Emerging principles
    - Intent, notice, opportunity to review
    - Attribution/authentication
    - Record integrity/audit trails
- Key regulatory issues
  - UDAPP/ non-bypassble?
  - Compliance/timing of disclosure and delivery
  - Tension between user friendly presentation and regulatory form requirements
Illustration – digital delivery of documents

**Delivery Design Choices**

- Secure or unsecure?
- Push out in email/SMS, or send “ready notice” and pull behind firewall?
- Embedded hyperlinks in “ready notice” email?
- Permit target to set delivery preferences?
- Permit target to designate multiple recipients?
- Forced review or bypassable?

**Design**

- Enrollment / consent process
- Audit trails and reporting
- Transmittal message contents
- Authentication process for access to secure data (if applicable)
- Record generation and posting to delivery system
- Message or notice generation/transmission
- Record retention/destruction process
- Record generation/posting

**Execution**

- Establish agreement on delivery
  - When deemed delivered
  - Delivery address
  - Obligation to update address
- Obtain ESIGN consent
- Generate records
- Send notice or attachments
- Provide opportunity to retain
- Generate audit trail
- Handle bouncebacks
- Handle withdrawal of consent

**Key Considerations**

- Will the records contain sensitive information?
- How will cross-system compatibility/communication issues be addressed?
- Are there “phishing” or “pharming” issues to address?
- Need to maintain control over display and audit trails?
- Need to obtain ESIGN consumer consent?
- 2-factor authentication required?
- How much of design will be automated or manual?
- Is system intended for use with targets without prior electronic relationship with sender?
- Regulatory requirements for timing, delivery, proximity, conspicuousness, forced review?
Other legal and regulatory considerations when communicating with customers in the digital channel

- **Americans with Disabilities Act (ADA)**
  - No federal regulatory standards exist for website accessibility; de facto standard is WCAG 2.0 AA
  - Two main sources of private risk: (i) Demand letters seeking money and fees and (ii) courts starting to require companies to meet WCAG 2.0 AA standard
  - Interaction with Section 255 of the Communications Act and Twenty-First Century Communications and Video Accessibility Act

- **CAN-SPAM Act**
  - Develop compliant opt-out process for marketing emails that is nimble enough to ensure that customer not inadvertently opting out of all emails (EG, non-marketing emails)
  - Ensure not using false or misleading header information or deceptive subject lines
  - Ensure compliance with FCC’s consent requirements for sending mobile service commercial messages
Other legal and regulatory considerations when communicating with customers in the digital channel (cont’d)

- **TCPA**
  - Consent requirements for calls made using an autodialer, prerecorded, or artificial voice to a cellphone unless wireless carrier does not charge called party for call. Prior express consent for informational calls; prior express written consent for telemarketing
  - Prior express written consent needed for telemarketing calls made using prerecorded or artificial voice to a residential line
  - National DNC list requirements for telephone solicitations; company-specific DNC list requirements for telemarketing calls
  - Autodialer definition still unclear, but recent federal court decision rejected expansive FCC definition. FCC recently sought comments on autodialer scope
  - Re-assigned numbers: FCC exploring solutions. Companies can take steps to mitigate risk
Other legal and regulatory considerations

- **ePayments**
  - Many ePayment solutions are subject to strict requirements for consumer authorization and disclosure, notice of transactions, representations and warranties by payees, limits and controls on practices, and investigation/correction of unauthorized transfers. Exposure for violations includes actual damages, automatic transaction reversals, statutory penalties (individual and class action), and regulatory enforcement.
  - Applicable rules, which frequently overlap and sometimes conflict, include Regulation E, NACHA Rules, card network rules (VISA, Mastercard, etc.), money transmission licensing, Regulation CC, AML/BSA and others. Innovative solutions are often necessary in order to “thread the regulatory needle” when taking and processing online and mobile payments.

- **Data collection, use, sharing, securing**
  - Data use, tracking/geolocation, biometrics, and data security are subject to both state and federal requirements – including Regulation P, the California Consumer Privacy Act, state data privacy and security laws.
  - Opportunities and challenges of artificial intelligence.
  - GDPR and the possible termination of the US-EU Privacy Shield agreement may impact policies and practices of US companies with respect to data retention and sharing with third parties.