Understanding Compliance Pitfalls Under the Updated TCPA

Alex Krylov, CIPP/US, CIPM
Privacy and Compliance Manager

Agenda

- Context
- Compliance landscape
- Tough questions
- Putting it all together

THIS IS NOT LEGAL ADVICE

To mitigate risk to your business, please consult with appropriate legal counsel about your particular situation.

Context

How the TCPA is impacting marketers and their service providers.

TCPA litigation on the rise

- **TCPA Private Right of Action**
  - "Spammed" consumers can sue SMS senders without first demonstrating harm
  - Can seek injunctive relief which can disrupt business practices
  - Can seek recovery of actual monetary loss, or
  - Courts can issue statutory damages of $500 - $1500 (max) *per violation*
  - Max penalty if alleged violations willful or knowing

- **Liability arising from client use of SMS services**
  - Direct consumer claims against service provider
  - Indemnity obligations to clients for consumer TCPA actions (specifically class action suits)

- **10,000** spam texts
  x
  $500 per violation
  ==========
  $5mm in damages (plus additional legal fees).

The biggest risk

Sending SMS messages without consent

- Most of the well-known US SMS lawsuits were brands that were accused of sending texts to recipients that never overtly opted in
- When a user texts Stop to a short code, they should get a confirmation text that they will no longer receive any text messages
- Even if the law allows a “reasonable amount of time” to stop sending messages to that user, the texts should stop immediately
- Due to the more intimate and high visibility nature of SMS, users are far more likely (than email) to complain to the client or their carrier if they feel they are being spammed

Compliance traps

Tough questions SMS senders and service providers should ask

Are you protecting yourselves and each other?

- **Senders**
  - How are you obtaining subscribers?
  - Is your express consent “compliant”?
  - Can you prove *written* consent?
  - Are you retaining consent records?

- **Service Providers**
  - How do you onboard clients?
  - Do you have policy controls in place?
  - How robust are your technical controls?
  - Your contractual controls?

Compliance landscape

Overlapping regulatory and self-regulatory requirements.

TCPA before the update

- Enacted in 1991 to address aggressive telemarketing practices
- Regulates calls or transmissions made using an automatic telephone dialing system (ATDS)
- Mostly an **opt-out regime**
- Marketers may rely on a pre-existing business relationship (EBR)
- Consumers can sue alleged violators in court
- Short Code-based text messaging programs a grey area

TCPA after the update

- Effective Oct 16, 2013, Updated July 10, 2015.
  - Eliminates ‘implied consent’ through a existing business relationship (EBR)
  - Unambiguous *prior express written consent* for “marketing” text messages
  - *Oral or written* consent for informational texts
  - New disclosure requirements for recurring text messaging programs
- Consumers **can still sue** alleged violators in court

- **Min** $500 – max $1500 penalties *per violation*
- Fertile ground for lawsuit trolls

FCC Declaratory Ruling and Order
July 10, 2015

- Confirms text messages are the same as telemarketing
- Broadly defines “autodialers” to include martech,
  - Concerns with marketers “using a random or sequential number generator” to send bulk SMS spam
- Creates a “safe harbor” for reassigned numbers as consumers increasingly jump carriers
- Customers can revoke consent at any time in any reasonable way, including orally
- “Single interaction” and certain “free to end user” programs exempt

- Ruling provides little relief to marketers complying with industry best practices

CTIA self-regulatory requirements

- Disclose program name, product type, Short Code
- Obtain separate express consent for unrelated messages
- Obtain user-initiated express consent
- Confirm web-form subscriptions with Double Opt-In
- Specify if recurring messaging (E.g. 3 msg/wk)
- Disclose inherent cost “Msg & Data Rates May Apply” adjacent to Call to Action
- Provide easy access to T&Cs and Privacy Policy
- Instruct how to get HELP (more info); how to STOP (opt-out) from the handset

ctia Wireless Foundation™

MMA MOBILE MARKETING ASSOCIATION

Sender, is your consent "compliant"?

For web form and handset-initiated subscriptions.

Ways customers can opt-in to an SMS program

- Web form (special rules apply)
- Texting to a short code
  - In-store signage
  - Online ads or web page
  - Radio TV ads
- Verbally/offline
  - Paper application
  - Call center
  - Point of sale

CASL-like requirements

Consent must be "Unambiguous"

- A "clear and conspicuous disclosure" to the consumer that he/she will receive future texts/calls
- Consent may not be a condition of purchase (as applicable)
- Obtain consumer's written consent with signature
- Advertiser bears the burden of proof of compliant consent

Consent must be "Written"

- Electronic or digital forms of signatures are valid, including via email
- Website form, text message or voice recordings OK if compliant with E-SIGN Act

- No pre-checked boxes!
- "One-time" contemporaneous responses sent to consumer requests are exempt

  (E.g. "Reply Yes" request, coupon, receipt, etc)

Initial consent may be deemed invalid

Without the right opt-in language at CTA

- **No pre-checked boxes on web forms!**
- At *any* readable call-to-action:

  By texting JOIN to 12345 you consent to receive recurring marketing text messages from Brand X via automated technology to the mobile number provided.

  Consent is not required to purchase goods or services. Periodic messaging. Text STOP to cancel, text HELP for help. Message and Data Rates May Apply. TC/Privacy: http://bit.ly/348dw

- A "one-time" contemporaneous response to a consumer-initiated response may not violate TCPA (E.g. a Double Opt-In request)

- **Best practice:** Have the consumer initiate engagement using their handset.

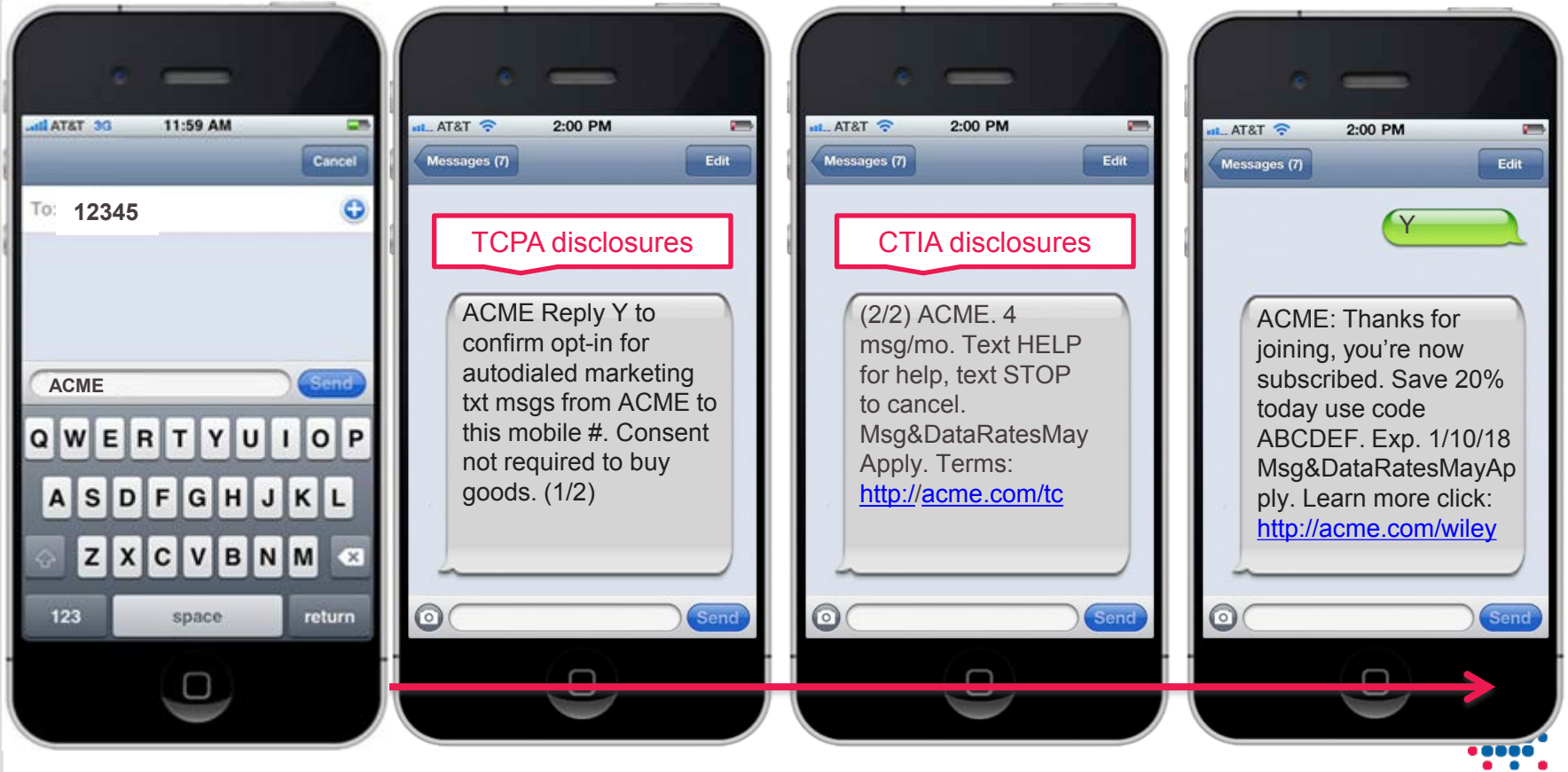
Sender, can you prove *written* consent?

Double Opt-In can strengthen consent records

- Not required by law but is a long-standing best practice
- Multi-step validation for all subscriptions
- Safeguards in the process prevent fraudulent, inadvertent or accidental sign-ups
- Generates contemporaneous electronic records of user interaction.
- Success or failure tracked in platform to the nanosecond
- **Best practice:** Send a DOI request within 12-18 hours after collecting mobile number

Single Opt-In **Double Opt-In**

Example conservative DOI flow



Sender, are you retaining consent records?

What should I be keeping?

Let's take a page out of the CRTC's CASL playbook

- An SMS sender should consider maintaining hard copy and/or electronic records of the following:
  - Commercial electronic message policies and procedures
    - Staff training documents
  - All evidence of prior express written consent from consumers who agree to receive marketing or recurring text messages
    - Acquisition campaign records
    - Message scripts and T&C language
    - Initial Opt-In logs; Double Opt-In logs preferred!
    - Timestamps!
  - All contemporaneous unsubscribe requests and resulting actions

- **Best practice:** Maintain records of consent for at least four (4) years. (statute of limitations under the TCPA)

Example Double Opt-In logs

ID	Create Date	BTN	Carrier	Approved	IP Address	Product Code ID	Campaign ID	Opt-In Type	Campaign Type
12345678	3/2/17 9:45:52.360 AM	9171234567	Verizon	1	**98.765.432.1**	1000	0001	**Handset**	In-Store

BTN	Message Flow	Create Date	Message	Delivery Status
9171234567	MT Message	3/2/17 9:45:52.397 AM	ACME Reply Y to confirm opt-in for autodialed marketing txt msgs from ACME to this mobile #. Consent not required to buy goods.	SUCCESS

Create Date	BTN	Response
3/2/17 9:49:54.337 AM	9171234567	**Y**

9171234567	MT Message	3/2/17 9:49:54.450 AM	ACME: Thanks for joining, you're now subscribed. Save 20% today use code ABCDEF. Exp. 1/10/18 Msg&DataRatesMayApply. Learn more click: http://acme.com/wiley	SUCCESS

Provider, are you managing your own risks?

Armor up with these service best practices!

- **Policy:** Set Double Opt-In as the default for all recurring text messaging (SMS) programs;
- **Contract:** Obligate DOI; revise SMS agreements to improve indemnity and insurance language
- **Vendor Migrations**: Check that client retrieved consent records from previous SMS service provider
- **Onboarding Diligence:** Request evidence of TCPA-compliant CTAs, T&Cs and consent records
- **Scrubbing:** Automate delivery of and scrubbing against “deactivated” and “transferred” phone number reports from carriers
- **Opt-outs:** Enhance infrastructure reliability and implementing endpoint monitoring to ensure opt-outs are processed
- **Assurance:** Set up regularly recurring audits of SMS programs under management
- **Education:** Help clients understand TCPA vs CTIA requirements and non-compliance risks

Bear trap: ‘orphaned’ SMS subscribers

Re-engagement or reconfirmation efforts carry TCPA risk

- If client finds a subscriber list sitting on a shelf or
- If client does not have records of compliant consent
  - **Low database risk, high compliance risk.** Do not reconfirm or re-engage. Send existing contacts intended broadcast messages.
  - **Moderate database risk, high compliance risk.** Send existing contacts a welcome message with a permission pass (opt-out option).
  - **High database risk, moderate compliance risk.** Send DOI (Reply Y) request to existing contacts. Onboard only net respondents.
  - **High database risk, low compliance risk.** Send DOI (Reply Y) request by email to existing contacts with email address on record.
  - **High database risk, no compliance risk.** Burn existing contact lists. Start from scratch when onboarding and setup is complete with CCM.

Putting it all together

Protect yourself, protect your clients

Avoiding surprise headaches

- **Governance**
  - Enhance contractual indemnity and arbitration controls
  - Set DOI as your consent baseline for SMS
  - Educate clients upfront on TCPA vs CTIA requirements, litigation risks, and their obligations
  - Store consent records for 4 – 5 years
- **Business**
  - Enhance onboarding process to ensure all lists have valid prior express written consent
  - When migrating clients, request and import consent records from other provider
  - Lock administrative text message templates to prevent tampering
  - Send automated messages confirming opt-out
- **Technical**
  - Automate end to end monitoring to detect messaging anomalies
  - Enhance infrastructure to ensure opt-outs/ins are always processed asap
  - Process nightly carrier ported and disconnect number files