# From Vulnerable to Vigilant

## Marketing Security and Trust Building Made Simple


October 2025

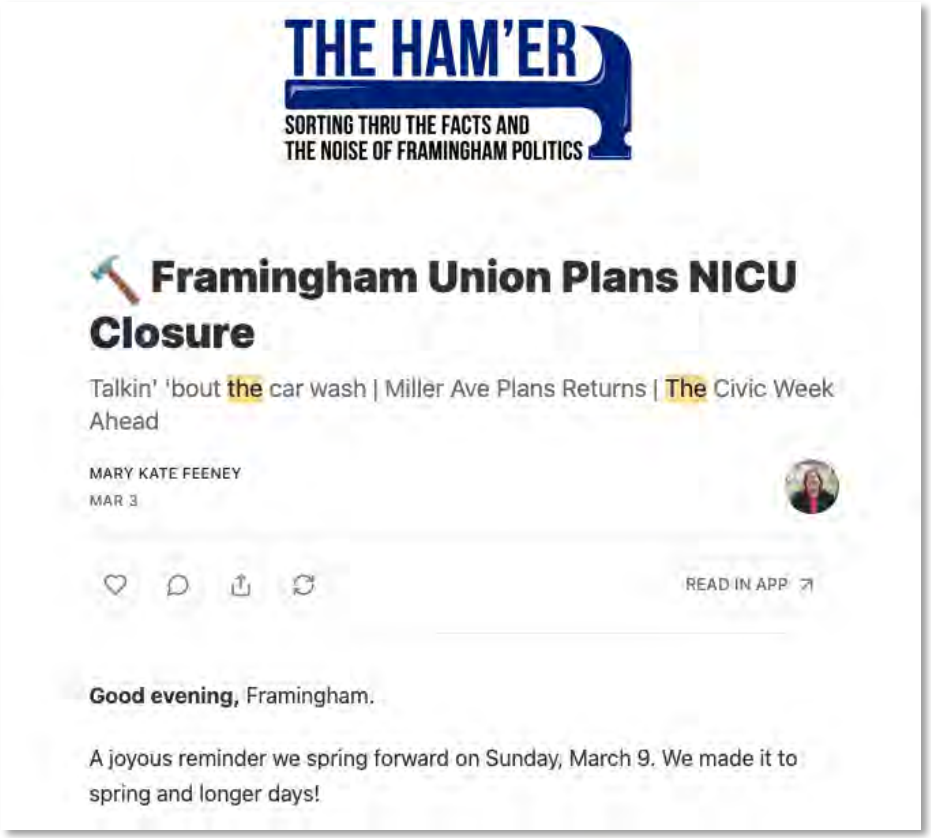
Mary Kate Feeney

mk@docksidemedia.co | www.docksidemedia.co

dockside MEDIA

# Who am I?

- Creative Principal of Dockside Media
- Writer of ***The Ham'er*** – a weekly email about Framingham politics
- Managed online communications for the Office of the Governor
- Ghostwriter and marketing strategist




dockside MEDIA

# Quick Question

Have you ever hesitated before posting something online, thinking...

***"Should I really share this?"***

That gut feeling? That's your internal security system working.

Today, we're turning that instinct into a simple system you can use every time you market your business.

dockside MEDIA

# The Challenge

We all want to be:

- Authentic
- Relatable
- Engaging

But in the rush to connect with customers, it's easy to accidentally share too much.

That can cost you trust, money, or even legal trouble.


dockside MEDIA

# What You'll Learn Today

- ✓ Three simple filters to run your marketing through
- ✓ Real-world examples of what can go wrong
- ✓ Quick fixes you can implement today
- ✓ Content strategies that build trust while keeping you safe

dockside MEDIA

# The Three Big Risks

Before you post, ask yourself:

Could this create a legal problem, a security hole, or damage trust?

# Risk #1 – The Legal Landmine

**What it looks like:**

- Sharing customer photos without permission
- Using client names in testimonials without consent
- Posting "before and after" images with private information
- Making health, financial, or outcome claims you can't back up

# Example: The Salon

**The Story:** A local salon posted amazing before-and-after hair photos on Instagram. Great marketing, right?

**The Problem:** They didn't get written permission from the clients. One client was going through a divorce and didn't want her image online.

**The Result:** That post led to a legal complaint and damaged the salon's reputation.

**Quick Fix:** Create a simple photo/testimonial release form. Keep signed copies on file. When in doubt, ask permission—every single time.

dockside MEDIA

# Risk #2 – The Security Slip

## What it looks like:

•Posting "We're closed for vacation July 10-20!"—advertising an empty building
•Sharing behind-the-scenes photos with passwords or security codes visible
•Announcing big inventory deliveries or cash-handling details
•Geotagging posts from your home when you work remotely

dockside MEDIA

# Example: The Trade Show

**The Story:** A small retail shop owner posted a cheerful "We're at the trade show in Vegas all week!" message.

**The Problem:** While they were gone, someone broke in.

**The Result:** The insurance company questioned the claim because the business had publicly announced the building was empty.

**Quick Fix:** Schedule posts to go live during business hours. Review photos carefully—zoom in and check backgrounds. Never announce when your business is completely unattended.


dockside MEDIA

# Risk #3 – The Trust Breaker

## What it looks like:

- Oversharing about client situations, even without names ("Just helped a client who was going through a tough divorce...")
- Sharing data dashboards or analytics that include customer information
- Posting screenshots of emails or messages without blurring names
- Being vague about how you handle customer data ("We keep your info safe!")

dockside MEDIA

# Example: The CPA

**The Story:** A CPA posted on LinkedIn: "Just helped a local business owner save $40K on taxes!" Sounds great, right?

**The Problem:** The local business community is small. People started guessing who it was.

**The Result:** The client felt exposed and took their business elsewhere.

**Quick Fix:** Ask yourself: "Could someone figure out who this is?" When in doubt, make details more generic or get explicit permission to share specifics.

# The Simple Filter System

## Three questions to ask before you post anything...


dockside MEDIA

# #1: Would I want this shared about ME?

## The Empathy Test

If you wouldn't want your accountant posting about your business challenges (even anonymously), don't post about your clients' situations.

Put yourself in your customer's shoes.

# #2: What could someone DO with this info?

## The Security Test

Look at your post through the eyes of someone with bad intentions.

Could they:

- Know when you're not there?
- See sensitive information in the background?
- Figure out your security systems or processes?
- Identify vulnerable customers or situations?

# #3: Can I prove this or do I have permission?

## The Legal Test

- Making a claim? Have the data to back it up.
- Sharing a photo? Have written consent.
- Mentioning a client? Have their explicit okay.
- Using a testimonial? Keep that permission on file.

# The Golden Rule

**If you answered “no” or “I’m not sure” to ANY of these questions…**

**DO NOT POST IT!**

dockside MEDIA

# Build Trust the Right Way

- **Use trust signals in your marketing:**
  - "We never share your information with third parties"
  - "Your data is encrypted and secure"
  - "All photos shared with written permission"
- **Show, don't just tell:**
  - Add a simple privacy statement to your website
  - Include "We respect your privacy" in email signatures
  - Display security badges if you have them
- **Be transparent about processes:**
  - "Here's how we protect your information when you work with us..."
  - "Your consultation is always confidential"
- **Create a simple social media policy for your team:**
  - What can be photographed
  - What needs permission
  - What should never be posted

dockside MEDIA

# Transparency and Education

- ✓ Explain the "why" behind your policies
- ✓ Educate customers on how to protect themselves
- ✓ Share how you chose your security tools or vendors
- ✓ Position yourself as a trusted advisor, not just a seller
- ✓ Create helpful content that builds expertise

# Social Proof Done Right

- ✓ Respond to ALL reviews professionally
- ✓ Show credentials and certifications (years in business, memberships, awards)
- ✓ Display third-party validation (BBB rating, industry associations)
- ✓ Share media mentions or speaking engagements
- ✓ Never reveal client details when responding to criticism

dockside MEDIA

# Quick Wins You Can Implement Today

1. **Review your last 10 social media posts** Would any of them fail the three-question filter?
2. **Take down anything questionable** Better safe than sorry
3. **Run future posts through the filter before publishing**

# Additional Action Items

1. **Create a simple permission form for photos and testimonials** Template: "I give [Business Name] permission to use my image/words in marketing materials. Signed/Dated."
2. **Audit your website and email templates** Add one clear privacy statement if you don't have one
3. **Take 5 minutes before posting anything** Run it through the filter: Would I want this shared about me? What could someone do with this? Do I have permission/proof?

# Remember

Security isn't about being secretive or boring in your marketing.

It's about being intentional.

Your customers are paying attention to how you handle their information—make that a competitive advantage, not a liability.

# Questions?

## Contact Information:

- Email: mk@docksidemedia.co
- Phone: 508-733-3153
- Website: www.docksidemedia.co

dockside MEDIA