SPRING
Media Solutions

January 2026

BANK MONITOR MINUTE

The Latest in Social Media Compliance for Banks

By: Monte C. Williams | CEO

Key Takeaways:

- **Not all social media scams appear as comments or replies**
- **Impersonation tactics are becoming quieter — and harder to spot**
- **Examiner risk isn't about intent, it's about visibility and oversight**
- **UGC remains one of the largest blind spots in social media compliance**

> *This was one of those moments where you realize the risk didn't change, the tactic did. And that means our assumptions have to change too.*
>
> *Jill D. Williams*
> Founder Bank Monitor

THE BANK SOCIAL MEDIA SCAM BANKS DIDN'T SEE COMING

WHAT WE ARE SEEING

Most banks are familiar with spam comments and bot replies appearing on social media posts. That activity is disruptive, but at least it's visible; there's something concrete to review, remove, and document.

In December, we observed a **different tactic**.

Instead of replying to a customer comment, a scammer created a fake Facebook page designed to closely resemble a bank's official page, including logo and branding, and **simply liked the customer's comment.**

There was no public reply. No link to remove. Nothing obvious in the comment thread to review.

But when the customer received the notification, it appeared to come from the bank, and the page name included a message suggesting they had "won" something.

Why This Matters

This type of activity works because it avoids the places banks traditionally monitor.

Banks don't review every "like" on their social media pages, and examiners don't expect them to. But when impersonation activity appears connected to a bank's page, it can still create **customer confusion, reputational risk, and examiner questions.**

During examinations, the focus is rarely on whether the bank created the content. Instead, examiners want to understand how third-party activity is monitored, escalated, and documented, especially when it's visible on a bank-controlled channel.

What Banks Should Review Now

- How user-generated activity is monitored beyond visible comments
- How impersonation attempts would be identified if they don't involve replies
- Who is responsible for review and escalation
- Whether monitoring and remediation actions are documented consistently

One More Thing to Consider

In this case, there was nothing obvious to flag, yet a customer still saw what appeared to be a bank-branded interaction suggesting they had won something.

That distinction matters.

Scam tactics are increasingly designed to blend in, not stand out. Understanding how and why this worked is key to preventing the next variation, which may be even less obvious.

How This Story Ends

Once the impersonation account was identified, it was immediately added to our **Bad Actor list.**

That step didn't just block the account for the bank involved; it prevented the same impersonation from interacting with **any** of our bank clients' social media pages going forward.

That's an important distinction.

Scam activity rarely targets just one institution. These accounts are often reused, renamed, and redeployed. Treating them as isolated incidents leaves other banks exposed to the same tactic.

When something new appears, the goal isn't just to remove it, it's to make sure it doesn't show up again.

The Takeaway

User-generated content risk isn't static. The tactics change, and effective oversight has to change with them.

The strongest programs don't just react; they **learn, adjust, and strengthen** protections across the board.

That's what examiner-ready social media compliance looks like in practice.

Want the full story?

Read the real-world breakdown of how this scam unfolded — and why it matters for banks.

👉 https://springmediasolutions.com/social-media-scam-banks-didnt-see-coming/

Have Questions About Your Own Social Media Oversight?

📩 **Email:** monte@springmediasolutions.com
📩 **Email:** jill@springmediasolutions.com
📞 **Call/Text:** 318.243.1076
📅 **Schedule Your Free Social Media Compliance Assessment**

Trusted by banks. Built for examiners. Managed by experts.