BankersOnline.com

When Social Media Attacks
by Barry Thompson, BOL Guru
Guru Bio

The CEO pulls into the bank's parking lot to find angry protestors lined up and carrying signs warning customers to bank elsewhere. As he reaches the main door, reporters push forward to interrogate him regarding comments recently made about his bank on social media websites. When he finally gets inside the bank, the first question the confused CEO asks his staff is, "What the heck happened?"

Our CEO has just discovered the power of social media. Up to this point, he has been discouraging his institution from establishing a social media presence, only to find that social media has now been used against him in an attempt to discredit the institution.

Using Facebook, Twitter, or LinkedIn is an effective way to connect millions of people cheaply and easily, yet some institutions are afraid of taking that first step into the world of social media. But whether they know it or not, and whether they like it or not, they're already there.

If you have staff members under the age of thirty (or staff members who use social media at any age), your organization is already in play. For example, somewhere on the Internet, your staff members have already identified themselves as your employees, perhaps mentioning their job titles online, and sometimes even describing their daily duties. Your account holders are also already there making comments about your service, and sometimes even making their account numbers visible online.

If you still think you can avoid social media, let me assure you: That time has passed.

Many articles have been written about the benefits of utilizing social media, but few describe how it can be used to attack your financial institution. Yes, most people use social media for benign reasons: to tell the world about their day, where they went on vacation, or even what they're having for dinner. Some people, however, will use social media to tell the world about how you have "wronged" them.

Every financial institution has a system in place to handle account holders' complaints, but pressure from users of social media will force you to institute a system that guarantees you go above and beyond to handle every account holder's complaints immediately and effectively - or else. Of course, most institutions probably think they already have a good system in place, but now is the time to take a second look at what you do.

For example, on consulting assignments I've encountered frontline staff members who didn't know to whom they should report various problems, who didn't know how to handle an upset account holder, and who didn't know if they even had the authority to question a person's transactions. I've also encountered management who felt they weren't obligated to report problems because they were "decision makers" who didn't feel the need to follow established procedures.

With this in mind, let's review some simple situations that could escalate into a full-blown social media attack:

- A customer believes the financial institution has mistreated him in some way
- An account holder has had money removed from her account in error
- A repossessed car ends up being the wrong car, or it was repossessed on the same day payments were brought current
- A shareholder decides the bank's management is overpaid
- A check clears that had a stop payment placed against it eight months ago. The staff member who usually handles these situations is on vacation, so the one person on your staff for whom you wouldn't select this duty explains the problem to your upset account holder -- only the explanation isn't phrased diplomatically

In the past, customers who found fault with an institution might demand to talk to the manager; call the main office; or in the worst-case scenario, retain a lawyer. But most unsatisfied customers would simply walk away angry at the bank for years to come, informing maybe seven to ten family members or friends about what happened. Today, those comments will be posted on social media websites, where thousands (potentially even millions) of people will have access to them. In fact, "Bank Transfer Day" was created by a disgruntled Bank of America customer who encouraged 500 of her closest Facebook friends to transfer their accounts to credit unions, and the Facebook page she created for the event subsequently received 54,900 "likes." Perhaps not coincidentally, on November 5, 2011, the day scheduled for the event, 40,000 people opened new credit union accounts. This incident has become a case study for anyone who is considering publicly attacking a financial institution.

The customers who are most likely to launch this kind of attack will take a passive-aggressive approach. These customers will let someone know they're unhappy, or maybe even write a letter to the CEO. But if they're dissatisfied with your response, they won't just walk away. They'll study your bank from a distance, performing background checks on management, looking for donations the bank made to groups that don't have a positive image within the local community, or befriending your staff members on social media websites in order to uncover some kind of vulnerability.

When they discover your weaknesses, they'll expose them on social media websites accompanied by a call to action. For example, if a senior manager of your institution has faced a DWI charge, lied about his/her accomplishments, received special treatment, or made some other mistake, the attacker has hit the jackpot. Every person reading this article knows about some incident their financial institution would rather not have publicized. This is the piece of information our attacker is looking for to initiate an attack.

Once these attackers post that first bit of information on a social media website, they'll make a series of subsequent and related posts over an extended period of time as a way of hammering their message home. Thousands upon thousands of people might then be exposed to it. If properly executed, this tactic could force the financial institution to operate in crisis mode on a daily basis. Not knowing how to handle such an attack could cause the bank to lose account holders (by not responding properly or quickly enough to the charges levied against it), and the old standby solution of having a lawyer contact disgruntled customers might not work in this case for several reasons:

1. You don't know who these attackers are. If they are Internet savvy, finding them might take days -- if you can find them at all.
2. These attackers often retain attorneys in advance of the attack and know you may not have any legal grounds to stop them.
3. Attackers like this are often so mad that they don't care about repercussions. They know your reputation

will be severely damaged before you can hurt them.

It is important for every financial institution to establish a system for monitoring social media, and that customer complaints are all handled the same way. Frontline staff, call centers as well as management, must know how to report problems with no deviations from policy so no one can claim that they didn't know what/where/to whom to report. When an attack is levied against an institution, a response must be made quickly, honestly, and with an open offer to the aggrieved party to have a dialogue with you. You must know the full story of what happened and if this has ever happened to another account holder before you respond. A response asserting that it was an "isolated incident" when it actually wasn't will permanently ruin your credibility.

Although you may not think your institution is susceptible to attacks via social media, the fact is, the game has changed: If you don't monitor social media, social media will monitor you.

First published on BankersOnline.com 8/27/12