



# Social Media for your Community Bank

Barbara Zachariasen

11/27/2010



**Tweeting on Twitter,**

**Friending on Facebook,**

**Wikis,**

**Mashables,**

**Blogs,**

**Diggs,**



**Status updates**

Web 2.0 Applications and Online tools are growing by leaps and bounds. Social Media isn't just a term anymore, it is a movement. How we communicate is changing. Business and News updates in seconds. Talking with friends and family at any time, in any place. Networking or collaborating with clients and vendors at the touch of a button. How do we keep up?

Many of you have questions like: What is "social media"? Should we use it? How secure is it? How will it benefit our bank? At SBS, our primary focus is customer service and communication so we would like to answer your questions and help to make sense of some of the confusion.

SBS believes this situation presents both opportunity and risk. Guidelines and recommendations for using social media technologies in a manner that minimizes the risk should be utilized.



The decision to embrace social media technology is a risk-based decision, not a technology-based decision. It must be made based on a strong business case, supported at the appropriate level for each department or agency, considering its mission space, threats, technical capabilities and potential benefits. We offer the following information to help with this difficult decision.

# The social media terrain

There is a wealth of information about social media that exists both on and offline. We gathered a few definitions and facts that may help you better understand the terrain.

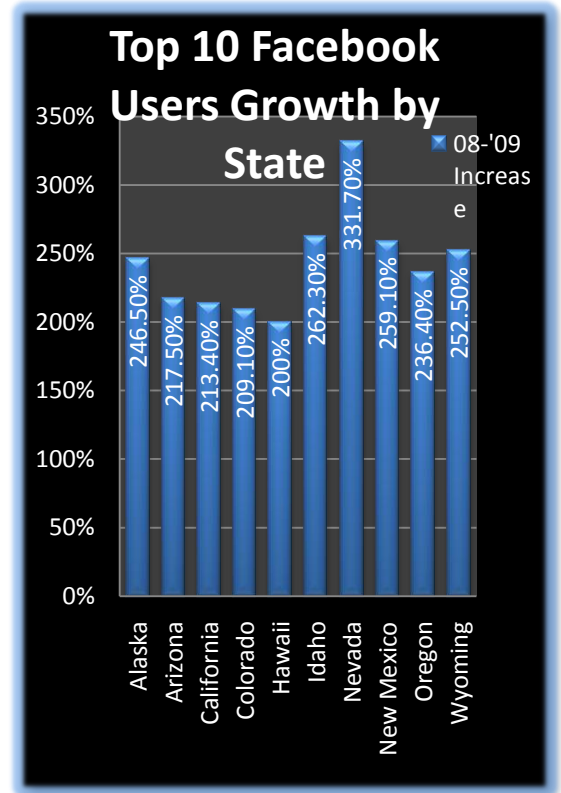


**Facebook** is a social networking website that was originally designed for college students, but is now open to anyone 13 years of age or older for amusement, marketing or research.

Facebook users can create and customize their own profiles with photos, videos and information about themselves or their companies. Friends can browse the profiles of other friends or and write messages on their pages.

## Facebook Facts

- **500 million** active users in July 2010
- **50%** of active users log onto Facebook on any given day
- More than **1.5 million** local businesses have active Pages on Facebook
- An average user spends more than **55 minutes** per day on Facebook
- **54% percent** of the companies studied have at least one Facebook Fan page (Burson-Marsteller, 2009)



**Blogging** is an online diary; a personal chronological log of thoughts published on a Web page; also called Weblog, Web log. Typically updated daily, blogs often reflect the personality of the author.

## Blogging Facts

- More than **133,000,000** blogs have been indexed since 2002.
  - **60%** of readers are 18-44
- **75%** of readers have college degrees and 40% have graduate degrees.
- **77%** of Internet users read blogs according to Universal McCann.
- **15%** of Bloggers spend 10 or more hours each week blogging.
- **56%** say that their blog has helped their company establish a positioning as a thought leader within the industry.
- **58%** say that they are better-known in their industry because of their blog.

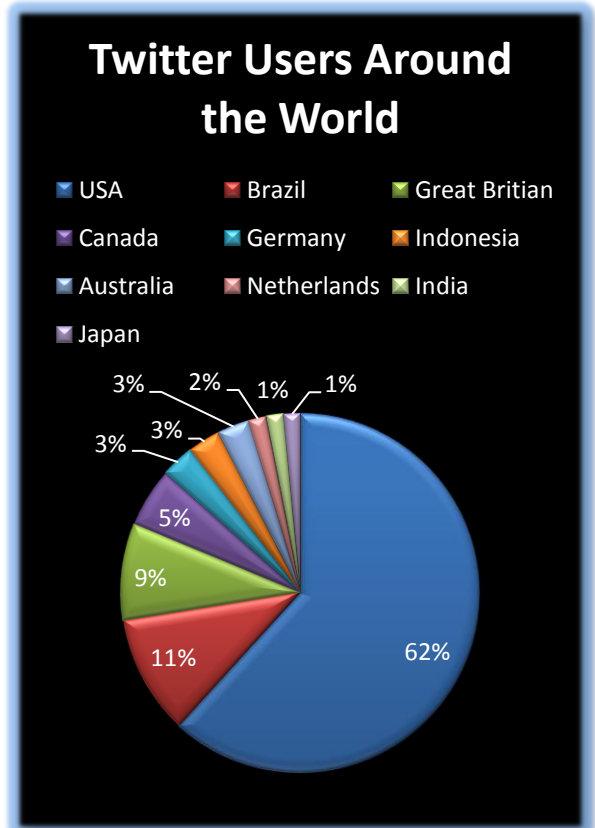


**Twitter** is a popular instant messaging system that lets a person send brief text messages up to 140 characters in length to a list of followers. Launched in 2006, Twitter was designed as a social network to keep friends and colleagues informed throughout the day. However, it became widely used for commercial and political

purposes to keep customers, constituents and fans up-to-date as well as to solicit feedback. Messages can be sent and received via cellphone text messaging (SMS), the Twitter Web site or a third-party Twitter application.

### Twitter Facts

- Twitter has **105,779,710** registered users
- It gets **300,000** new users a day
- Twitter now has **175** employees
- **600 million** search queries a day
- **75%** of traffic comes from outside Twitter.com
- **37%** of users update their status through a mobile phone
- **55 million** tweets per day or **640** tweets per second
- Twitter receives **180 million** unique visitors a month



**YouTube** is a popular Web video sharing site that lets anyone store short videos for private or public viewing. Founded in 2005, it was acquired by Google in 2006 for \$1.65 billion. Within a couple years, more than 25 quadrillion bytes (petabytes) of videos were being streamed from the site each month.

YouTube provides a venue for sharing videos among friends and family as well as a showcase for new and experienced videographers.

### YouTube Facts

- As of May 2010 – YouTube exceeds **2 billion** views a day
- By March 2010 **24 hours** of video is uploaded per minute
- The average person spends **15 minutes** per day on YouTube
- The number of advertisers using display ads on YouTube has increased **10-fold** in the past year

## Community banks are building a path

Facebook, MySpace, Twitter, YouTube, blogs and other social media are rapidly transforming how Americans congregate and communicate in the online and mobile setting. Leading financial institutions are blazing a path that will change how consumers interact with FIs and gain an increasing measure of always-on, real-time control of their money. There are risks associated with being early to engage in social sites, but there is potential for high rewards for financial institutions and tech vendors that develop cutting-edge tools that tap into the potential of social networks for viral marketing, brand awareness, cross-selling, financial literacy, customer service, consumer forums, timely alerts and always-on interaction.

SBS has accumulated the following information to help you make an informed decision about Social Media in your workplace. Whether you choose an “allow” policy or a “deny all” policy, that policy should be based on sound statistics and proven practices.

### Why brave the traffic?

Many banks have started using social websites to help them with everything from healing the financial industry to promoting their latest credit cards. By embracing the most popular tools available, the industry has also been embracing the best of what social media culture has to offer, and smaller community banks seem to be leading the charge when it comes to social media innovation. These banks have tapped into the root of what social media means to the community, enjoying success in the way of returning real value for their institutions.

#### 1. Community Building

Focusing on customer service and adopting the personality of the people they serve, community banks and credit unions can really teach the big guys a thing or two about what it means to be close to customers. Community building is something that banks should be doing more of because many of the most important touch points in our lives from attending college, to buying our first cars and building a home, to starting a business and saving for retirement all involve a relationship with a bank.

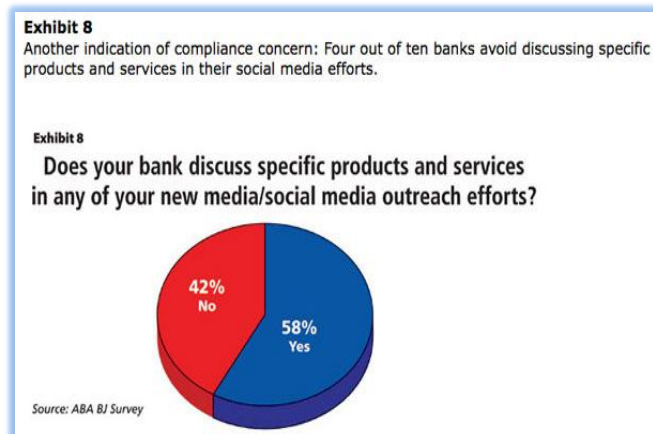
#### 2. Product Research

Whether you’re crowdsourcing to find out what customers think of your services or using social media as one tool in your arsenal to enlist customers to help develop new products, a social network is an undeniably powerful research and development resource.

#### 3. Customer Service

Social media has become a great customer service tool across many industries and banking is no exception.

However, not all banks are so proactive. A study done by the American Bankers Association found that four out of ten banks polled said that they avoid discussing specific products and services in their social media efforts.

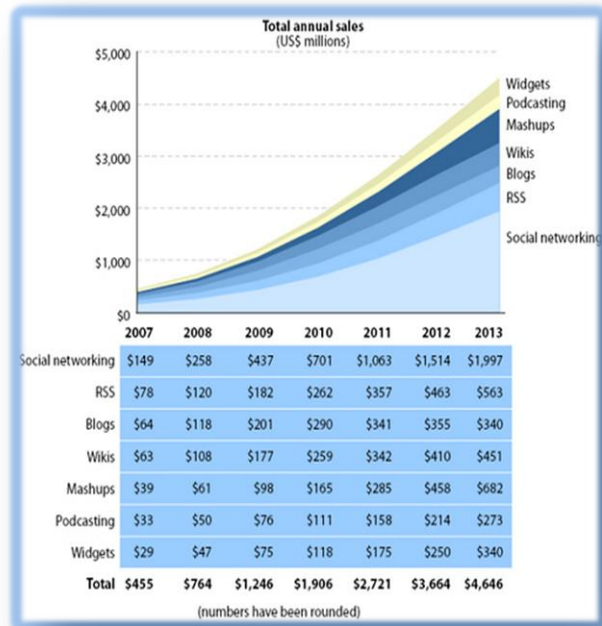


#### 4. Marketing & Promotion

Banks that are using social media to brand themselves or to market a specific product or service have found success by integrating social tools into their existing campaigns or creating new ones that capitalize on the spirit of the community. Whether it's by making the bank synonymous with solid financial advice or giving people the power to do some good in the world, banks have been finding that immersive marketing techniques using social media tools have brought solid results.

#### 5. Transparency

The financial crisis has led many customers to distrust banks, which is one reason why many banks are now turning to social media as a way to become more transparent to customers and build trust. David Armano, Senior Partner at Dachis Corporation, says that banks are like every other institution facing the evolution of the networks and websites providing empowerment to individuals and that they must adapt to join the conversation. "Banks also dealing with trust issues may accelerate that change," he said.



"Banks could potentially miss opportunities to mitigate risk ... by choosing not to participate in social media," said a bank spokesperson. "As a result, we recognize the value of a controlled and closely managed approach to social media as one of the many ways that we can be transparent with our customers and prospects."

**62%** of financial advisors agree that social networking is here to stay, saying that social media will have a lasting impact on the financial services industry.

#### Beware of the hazards

Fear of compromised productivity, reputational damage, data loss and inappropriate behavior is leading many employers to introduce strict controls on staff access to social media sites.

"Security plays a key role in policy shaping discussions," Brett Wahlin, ISO at McAfee. Bring attention to the threats and risks associated with social media, which includes discussing one of the critical traits - that the information posted is online forever.

**54%** of U.S. companies have banned workers from using social networking sites while on the job. **19%** of companies allow social networking use only for business purposes, while **16%** allow limited personal use.

Robert Half Technology

Employees must realize that social media is a public and highly social forum where controls go beyond the limits of an individual's network, as friends of friends will typically send invitations and links. Again, business owners should be aware that social media companies are there to make money and will engage in some sort of data mining or selling of information, so "companies need to assume that privacy doesn't exist," says John Pironti, ISACA board member and president of IP Architects, LLC.

Security professionals should educate the business owners on the threats of using technology and the consequence of not having a policy in place by outlining potential risks associated and making it a risk conversation. More, community bank leaders need to be involved on a constant basis with IT to be proactive with foreseen and real-time social network changes that may pose risks, as well as high risk issues such as dubious links, phishing attacks and insider threat should immediately brought to security's attention.

**Areas are leading the race concerning Social Media in community banking:  
Brand Protection**

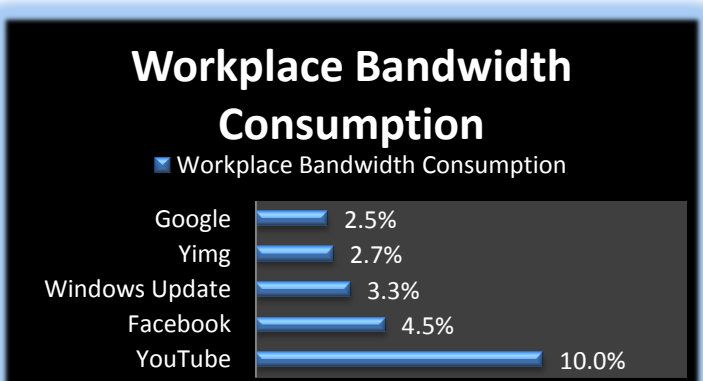
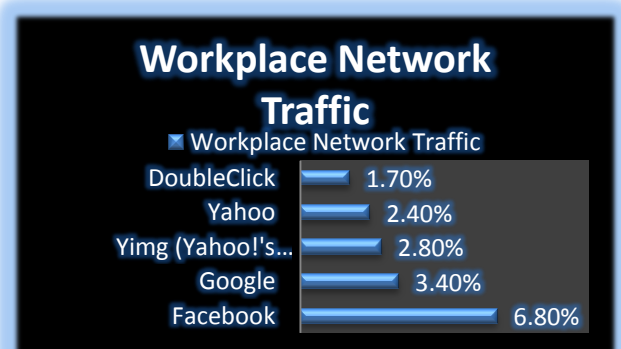
- **74%** of employed Americans surveyed believe it is easy to damage a brand's reputation via sites such as Facebook, Twitter and YouTube.
- **1/3rd** of employed respondents say they never consider what their boss would think before posting materials online.
- **61%** of employees say that even if employers are monitoring their social networking profiles or activities, they won't change what they are doing online.
- **54%** of employees say a company policy won't change how they behave online

**Risk Management & Compliance**

- **27%** of executives regularly discuss how to best leverage social networks while mitigating risks.
- **"You have to find a way to supervise this activity"** (FINRA Social Networking Podcast, 2009)

**Data Leakage**

- **17%** of US companies investigated the exposure of confidential, sensitive or private information via a posting to a social networking site
- **13%** of US companies investigated the exposure of confidential, sensitive or private information via a an SMS text or micro-blogging service (Twitter)



The effectiveness, however, of a social media policy ultimately boils down to organizations asking the question: **What is our policy on effective social media use at work?**

## The "must haves" when drafting a social media policy:

**1. Get User/Business Input** -- go to the users to ask them how they want to leverage this medium to promote their business goals. Clear expectations should be specified in terms of employee behavior, time spent and acceptable use of social media with personal and corporate accounts and these expectations should be aligned with other corporate policies with similar objectives like Internet use.



**2. Set a General Code of Ethics** -- providing guidance on the positive behavior expected from all employees regardless of channel. For instance, employees should be directed to act ethically and not divulge trade secrets or other valuable intellectual property.

**3. Establish Clear Rules of Engagement** -- that include an evaluation process for authorized communicators to know when they should and should not engage in a public dialog.

These rules spell out employee expectations in terms of tone, language to be used, as well as situations that demand an employee response like correcting misguided information related to interest rates or loans.

**4. Monitor** -- social media activity. How do employees use social media? How much time are they spending? Which sites do they visit? Who are their fans or followers? Answers to these questions are lead indicators for assessing risks and threat factors.

**5. Provide Training** -- on an ongoing basis. Social media is a powerful tool and comes with its own benefits and challenges. Companies should invest in adequate training programs to remind the users of their responsibilities and outline clearly what is acceptable and appropriate vs. not. Send frequent messages to employees on the misuse of social media. Draw upon case studies to understand the consequence of bad behavior or reputational damage to the company.

**6. Take Disciplinary Action** -- when necessary. Enforcement standards need to be set and implemented against employees that do not follow social media policy effectively. Example: when source codes are made public by employees or pornographic photos are posted.

## "Good Principles" as a roadmap

### 1. Maintain Confidentiality

Do not post confidential or proprietary information about your company, its customers, its management or your fellow employees. Use good ethical judgment and follow company policies and federal requirements

### 2. Maintain Privacy

Do not discuss a situation involving named or pictured individuals on a social media site without their permission. As a guideline, do not post anything that you would not present in any public forum.



### **3. Respect Company Time and Property**

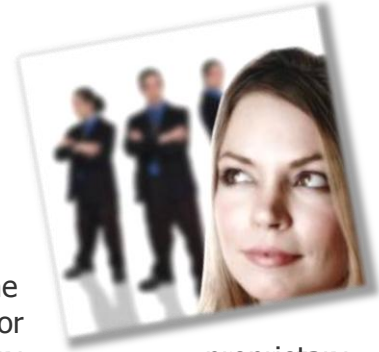
It may be appropriate to post at work if your comments are directly related to accomplishing work goals, such as seeking sources for information or working with others to resolve a problem. You should participate in personal social media conversations on your own time

### **4. Do No Harm**

Let your Internet social networking do no harm to the company you work for or to yourself whether you're navigating those networks on the job or off.

### **5. Understand Your Personal Responsibility.**

Staff and employees are personally responsible for the content they publish on blogs, wikis or any other form of user-generated content. Be mindful that what you publish will be public for a long time—protect your privacy.



### **6. Be Aware of Liability**

You are responsible for what you post on your own site and on the sites of others. Individual bloggers have been held liable for commentary deemed to be copyright infringement, defamatory, or obscene (as defined by the courts). Increasingly, employers are conducting Web searches on job candidates before extending offers. Be sure that what you post today will not come back to haunt you.

proprietary,

### **7. Maintain Transparency**

The line between professional and personal business is sometimes blurred: Be thoughtful about your posting's content and potential audiences. Be honest about your identity. In personal posts, you may identify yourself as a bank employee. However, please be clear that you are sharing your views as an individual, not as a representative of the company.

### **8. Correct Mistakes**

If you make a mistake, admit it. Be upfront and be quick with your correction. If you're posting to a blog, you may choose to modify an earlier post—just make it clear that you have done so.

### **9. Respect Others**

You are more likely to achieve your goals or sway others to your beliefs if you are constructive and respectful while discussing a bad experience or disagreeing with a concept or person.

### **10. Be a Valued Member**

If you join a social network, make sure you are contributing valuable insights. Don't hijack the discussion and redirect by posting self/organizational promoting information. Self-promoting behavior is viewed negatively and can lead to you being banned from Web sites or groups.

### **11. Think Before You Post**



Comments can be forwarded or copied. Archival systems save information even if you delete a post. If you feel angry or passionate about a subject, it's wise to delay posting until you are calm and clear-headed. Post only pictures that you would be comfortable sharing with the general public (current and future peers, employers, etc.).



## **Secure Banking Solutions**

### **Born out of a University's Excellence**

Secure Banking Solutions is the consulting spin-off from the National Center for Information Security at Dakota State University, a federally sponsored center for information security and the only center in the country dedicated to the protection of the financial infrastructure! Dr. Kevin Streff is the Director for the Center and also the founder and owner of SBS.

SBS offers comprehensive information security consulting to financial institutions. SBS is the general contractor helping institutions design and build their information security program. Other firms act like subcontractors taking on only pieces (e.g., IT audit, penetration testing, etc.). However, SBS takes responsibility for ensuring that financial institutions develop and implement strong information security programs. The SBS goal is to bring strategic guidance to equip clients to build their information security programs. We aim to fill the void on the management team where no one has IT security expertise. SBS understands that each financial institution is unique, but all desire to maintain and grow market share and serve their customers. Technology is an important factor in accomplishing those two objectives. As financial institutions use technology to meet their own unique personality and market, information security becomes increasingly important. Numerous high-profile information data thefts over the last year highlight how vital our country views this area.

SBS takes the time to get to know the management teams of their clients and how those teams seek to use technology to meet their marketplace needs. At the same time, SBS understands that having successful IT examinations from regulators is very important. These two needs guide our efforts. SBS assigns a team of consultants to each financial institution, which is headed by a lead consultant. When the team makes recommendations to management, they do it with an understanding of the institution's culture and personality.

### **General Info:**

[www.protectmybank.com](http://www.protectmybank.com)

Dr. Kevin Streff  
Founder and Majority Owner  
(605) 270-0790

Jeff Schreiner  
President and CEO  
(402) 686-0085

### **Sales Info:**

#### **Madison, SD Office**

Rick Olivier  
VP - Sales  
(605) 270-3321  
Jeff Haase  
VP - Business Development  
(605) 270-9854

#### **Mailing Address:**

1400 N Washington Ave Ste 103  
Madison, SD 57042-1147

#### **Philadelphia, PA Office**

Nick Podhradsky  
Regional Sales Representative  
(605) 770-3926

#### **Mailing Address:**

1001 Harper Ave  
Drexel Hill, PA 19026