

Growing use of Twitter among banks raises security concerns

A “friendly neighborhood banker in the Twittersverse” could be anybody... and anything but friendly

By Jeffrey Pilcher, CEO of The Financial Brand and ICONiQ, a financial branding consultancy. Pilcher regularly publishes insights on financial branding and marketing at his online publication, TheFinancialBrand.com.

The increasing number of banks exploring Twitter as a communications channel has sparked concerns over what security issues the online service might pose. Phishing attacks, identity theft, and the potential for people’s privacy to be compromised are among the risks troubling experts in the financial industry.

Twitter, a free social networking and micro-blogging platform that enables users to send and read messages (known as “tweets”), has seen U.S. growth explode past 25 million users, up from five million since the first of the year.

Banks are finding it difficult to resist Twitter’s power and popularity, and many are forging ahead despite security questions. Today, over 750 financial institutions have established an official presence on Twitter, a figure that has been steadily climbing over the last 18 months.

Keeping account information secure

Banks, including Bank of America and Wells Fargo, are using Twitter to help customers resolve service issues. At least one financial institution, Vantage Credit Union of St. Louis, Mo., provides basic account information such as balances and transaction history via Twitter.

“A number of financial institutions are using Twitter to widen and deepen their engagement with customers,” acknowledges Anamitra Banerji, a spokesperson with Twitter. “Many of them began by setting up their accounts and reaching out to users.”

Luke Owen with Truebridge, a financial marketing firm, says banks that use Twitter to engage with their customers must be careful.

“If you’re going to promote this channel as a customer service tool, you have to understand the risks,” he says.

Twitter exchanges between banks and customers about their accounts concern J.J. Hornblass, founder of BankInnovation.net. Hornblass is wary that sensitive information might be compromised, especially if someone publishes their banking details over an unregulated, third-party system like Twitter.

“There are risks for everyone,” Hornblass says, “including Twitter.”

Owen, on the other hand, hopes that bank customers share the responsibility to protect themselves. “Banks are taking the position that if a consumer is using Twitter, they should know better than to send a message out to the world that includes their bank account or other personal information,” he says.

Many banks tell customers to never divulge personal information on Twitter. Some have warnings posted on their Twitter profile pages, while others constantly publicly tweet reminders, such as Wells Fargo: “When u tweet, make sure u don’t share bank account info.”

Ed Terpening, vice-president for Social Network Marketing at Wells Fargo, testifies that he’s never seen customers share account information in the year or so that his bank has been experimenting with Twitter. “At most, we may see a phone number,” Terpening says. “And even then, we advise the customer to delete the tweet.”

“Protecting our customers privacy and security is incredibly important to us,” Terpening adds. “As Twitter changes and matures, it remains a constant concern.”

Fighting fraud and identity theft

One of the biggest Twitter security issues for banks hinges on the authenticity and legitimacy of accounts. How can someone determine if a Twitter account that claims to represent Bank X is truly something Bank X has sanctioned? For instance, how can Twitter users discern the difference between “Bank_of_America” and “BofA_Help,” both of which are active accounts on Twitter? Which one is the bank’s official account? BofA_Help may be the one officially approved by corporate, but how can people be sure?

One way BofA establishes the authenticity of its Twitter account is by cross-referencing their BofA_Help account on the corporate website. Clicking on the link displayed in BofA’s Twitter profile takes visitors directly to a special page on its main website that clearly identifies BofA_Help as one of the bank’s official communications channels.

The concern is that phishing attackers might make a lookalike account with only the slightest change: BofA_Helps or BofAHelp instead of the official BofA_Help. Impostors might try to pry sensitive personal information such as social security numbers—or worse, online banking passwords—from innocent customers who mistakenly assume they are dealing with the real Bank of America.

Verified Twitter accounts for banks

Twitter began verifying the accounts of celebrities like Shaquille O'Neill, Oprah Winfrey, and Britney Spears back in June 2009, saying they were looking to "establish authenticity of people who deal with impersonation or identity confusion on a regular basis." The move came in response to a lawsuit brought by Tony La Russa over someone impersonating the famous St. Louis Cardinals manager on Twitter.

Twitter doesn't reveal exactly how it determines the legitimacy of accounts, but the company does say it "contacts the person or entity the account is representing and verifies that it is approved." Twitter then places a special badge on the account's profile page declaring it a "Verified Account."

Currently, Twitter does not verify the accounts of financial institutions. Twitter's Banerji says Twitter is "planning the expansion of account verification to include businesses," but did not disclose the company's timetable nor what it might cost.

The verification of business accounts is part of a wider initiative Twitter has under way. Twitter is in the process of developing a suite of services as part of a commercial package. It will be the first revenue-generating product Twitter offers.

Banerji, who is managing the new commercial product for Twitter, did not provide details on what it may entail, although the offering is likely to include a bundle of premium services such as detailed analytics, in addition to verified account status.

"We are continuing to improve the process of account verification, which we began testing earlier this year," Banerji says. "We are also working on additional features that businesses have requested."

In an informal survey of financial professionals conducted by TheFinancialBrand.com, nearly all said the verification of accounts for financial institutions can't happen soon enough.

David Gerbino, a community banker and longtime personal Twitter user, thinks Twitter should start verifying accounts of financial institutions immediately and not wait on future plans for its commercial product.

"Anybody can create a Twitter account with any bank or credit union name," Gerbino points out. "Twitter should help its user base by verifying legitimate financial institutions. With all the fraud out there, every little bit of authentication in the financial space is helpful to consumers."

Phishing attacks affect financial firms

Verified accounts don't fix all of Twitter's security issues for banks, notes Paul Jonas, digital communications coordinator for the Independent Community Bankers of Minnesota. He fears what might happen if, for

instance, hackers gained control of a bank's account bearing the "Verified" badge.

"With verified status, the bank employees behind the accounts will have to be that much more careful to not fall victim to phishing attacks," warns Jonas.

While no financial institution has been directly targeted on Twitter—yet—he phishing attacks Jonas alludes to are more than just a theoretical possibility. Last month, at least two credit unions had their official corporate Twitter accounts compromised, with at least another three compromised since then. All five credit unions fell victim to a common—and quite successful—social-engineering dragnet whereby hackers send irresistibly narcissistic invitations directly to Twitter users: "Hey, is this you in this picture???" It's too funny!!!

The phishing message includes a link to a "spooft site," something that looks visually identical to the real Twitter login page. Any unsuspecting users who enter their account name and password are surrendering their Twitter information to hackers, who quickly hijack the account.

Future opportunities

Despite the security concerns Twitter presents, banks of all sizes—large and small—remain optimistic about the service as a channel to deepen engagement with customers in innovative ways.

"We believe Twitter holds promise as a means of helping our banking customers," a source within Citibank says. "We welcome any additional steps Twitter might consider to improve security and functionality for corporate Twitter accounts, because improving the customer experience is a win for everyone—our customers, ourselves, and Twitter." BJ

The electronic version of this article available at: <http://www.nxtbook.com/nxtbooks/sb/ababj0110/index.php?startid=26>