

BANK TECHNOLOGY NEWS



FRAUD

## A Text Alert for Community Banks

Bank Technology News | September 2009

This borders on invoking Murphy's Law: Most community banks haven't yet rolled out mobile banking, yet these institutions are the most likely to be hit by smishing, an emerging security risk that targets the mobile channel. And tech weapons have only limited powers to stop it.

"[Smishing] is like if I walked up to your door, introduced myself as being from a bank and asked you for your personal credentials. If you're foolish enough to give that information to me, there's nothing the bank can do about it," says [Joram Borenstein](#), senior manager of RSA, the security division of [EMC](#). "The only difference is smishing is happening through cells phones and PDAs."

Smishing is the perfect crime: Community banks have small IT staffs, low tech budgets, and SMS attacks of limited scope go largely unnoticed. "It's hard to blanket the entire U.S. with SMS; it raises a lot more attention. Community bank attacks are small and can fly under the radar," says [Patrick Peterson](#), a [Cisco](#) fellow and chief security researcher.

A smishing attack begins when crooks trick consumers into turning over personal information by sending dishonest text alerts to customers' mobile phones, often warning of fraudulent activity to mimic a security alert that an actual bank would send.

The victims then call a phony "bank" number manned by bad guys using open source asterisk software to set up fake voice operated customer service systems. Smishers blanket a specific area code with SMS text alerts, hoping to nab a high percentage of customers of a specific bank. For example, [Wescom Credit Union](#) and Farmer's & [Merchants Bank](#) in Southern California were targeted by smishers in July. [Merchants](#) - which ironically doesn't offer mobile banking, according to a spokesperson, put a warning on its Website. [Wescom](#), which also doesn't offer a full-fledged mobile banking program, nonetheless publicized that the "from" line in a smishing attempt has only a few digits, instead of a traceable 10-digit phone number. "A legitimate source of SMS will look different than an illegitimate one," [Peterson](#) says.

Smishing is closely related to vishing, in which fraudulent voice phone calls to mobile phones lure consumers into sharing credit card numbers or other personal data. RSA doesn't yet track smishing data, but it says that of the vishing attacks it's taken down in the U.S., 60 percent have targeted credit unions, community or regional banks, and [Borenstein](#) says that percentage should migrate toward 75 percent in the next year, a similar percentage as traditional phishing.

[Tom Wills](#), an analyst at Javelin Strategy & Research, says the best countermeasures are education, user-configurable mobile alerts and the use of mutual authentication, in which a bank authenticates itself back to the consumer before a banking session can begin.

[ClairMail](#) - which provides mobile payments and other financial services to a number of community banks including [Bank of Stockton](#), [Intercredited Bank](#) (FL) Alerus Financial (ND), City Bank of Texas and State Bank & Trust, ND (all of which integrate the infrastructure into their own back end systems rather than have ClairMail host the function) - deploys out of band multi-factor authentication, and also asks users to verify mobile transactions by answering simple "yes/no" queries. "You don't need to require a customer to provide personal information to verify a transaction," says [Joe Salesky](#), founder and chairman of ClairMail, adding certain transactions like a customer adding him or herself as a new payee are protected with one-time PINs. "If a customer calls or contacts a bank, it should be by using a number that's already known to the customer."

[mCom](#)'s platform monitors SMS activity for odd or "exceptional" use - such as an unusual number of messages sent to a device - that could be a sign that criminal are sending fraudulent texts. "The best thing that banks can do is not go into a defensive position when it comes to mobile banking," says [Serge van Dam](#), mCom's CMO. "Rather than justifying why mobile is secure, tell customers that mobile channels give them security because you can enable alerts for exceptional conditions."

[Firethorn](#), which hosts mobile banking and payment for all of its clients, registers consumers' mobile devices with a six-digit PIN and uses SSL to protect messages between clients and servers. And any transactional component, such as bill pay and funds transfers, are only available via downloadable platforms. "SMS is only a quick way to get information," says [Eric Kraar](#), manager of architecture for Firethorn, who also says education is still the primary deterrent to SMS fraud.

None of these strategies is foolproof, however. Even tech-driven protections such as dual authentication rely on consumers knowing the difference between legitimate and illegitimate bank communication. "As a bank, you should say 'here's what we do when an account is opened, here's now we notify you about activity on your account. You should ignore anything that doesn't look like this'," says [Justin Wykes](#), computer

crime specialist for the [National White Collar Crime Center](#).

---

© 2009 American Banker and SourceMedia, Inc. All Rights Reserved.

SourceMedia is an Investcorp company. Use, duplication, or sale of this service, or data contained herein, except as described in the Subscription Agreement, is strictly prohibited.

For information regarding Reprint Services please visit: <http://www.americanbanker.com/about/reprint-services-rates.html>