

# BANK SYSTEMS & TECHNOLOGY

Business Innovation Powered By Technology

## Three Ways to Deter Cyber Crime

By Contributor

By Joe Spatarella, *Online Banking Solutions*

**I**ronically, as businesses move from risky paper check payments to a safer means of electronic B2B payments, the online banking systems through which payments are originated have become an attractive fraud target. Although businesses are using payment fraud control devices such as ACH Positive Pay and ACH Debit Filter, they only mitigate fraud after it occurs. There are at least five fresh reasons to step up the security investment.

**1.** The browser is the weak point. Trojans and other malware like man-in-the-browser attacks that are difficult to detect hijack the transaction inside of a browser session, and subsequently attack the application and database on the server. According to FinServ Strategies, most of the top 100 banks have experienced similar incidents. Man-in-the-browser attacks are becoming mainstream, RSA reports in its whitepaper, "Business Success in a Dark Market: An Inside Look at How the Fraud Underground Operates," especially in the U.S. and Europe where two-factor authentication is already densely deployed.

**2.** The customer is the endpoint. Banks deliver services to business customers through the browser; however, they aren't in control of the business's computing environment. Businesses are legally responsible for their transaction banking environment, but 20 million U.S. small businesses are particularly vulnerable to cyber fraud as they don't have the experience or resources to combat fraud, yet they initiate high risk payments transactions (e.g., ACH, wires). Many banks provision online services to small businesses on consumer systems with inadequate security for business activity.

**3.** Tweet this - multichannel banking is here. The cyber threat environment is growing more complex, especially as Web banking expands from Web and file transfer to mobile/smart phone and social channels and as the workforce grows younger. An integrated multichannel approach to information, transactions and fraud is nec-

essary to lower costs and increase effectiveness.

**4.** Single sign on lags business banking. Banks are seeking new corporate/business portal solutions or independent SSO applications to solve the security usability problem. If the bank looks for an SSO solution in an existing packaged



online banking offering, it may not get the integrated authentication and entitlements it needs. "Most solutions secure the session," says Nick Owen of WIKID systems. As malware is now attacking at the application level, transaction authentication needs to be cryptographically distinct from the session.

**5.** Fuhgettaboudit - cyber crime is organized crime. According to RSA, Internet fraudsters have created an end-to-end supply chain to advance malware attacks and the online vector used to efficiently deploy them. While the security technology market is creating security-as-a-service solutions, criminals are creating fraud-as-a-service and fraud has moved from the consumer to businesses that initiate payments and bank online.

But new approaches are emerging to tackle 21st century online banking problems. Among them are the secure browser and integrated single sign on. Banks are taking three positive steps in the right direction:

**Organizing to combat fraud.** Business fraud incidents are significant (albeit under reported) as related by major security companies and members of industry entities such as the Financial Services-Information Sharing and Analysis Center. Formed by presidential directive in 1999, FS-ISAC, now has 4,100 members from institution, brokerage and insurance sectors. "Members successfully share threat vulnerabilities through a network of trust that guarantees anonymity, while reporting important threat information to finan-

cial industry, government and other industry sectors,” says FS-ISAC president William B. Nelson.

**Implementing secure browsers.** The secure browser solves the openness problem of the Internet without plunging the world back into private networks. Much like a dedicated business to bank connection, the secure browser uses only the rendering portion of the browser and restricts URL destinations with a bank and company controlled list through entitlements and self-tests for changes indicating malware such as Trojans. This creates a secure connection akin to a virtual private network, but without the technical requirements and cost overhead. Like a regular browser, the secure browser performs site authentication, but it shuts the user down if a site is not authenticated, rather than asking the normal user to decide whether it is okay to continue during an abnormal event.

**Using integrated, single sign on.** Independent integrated SSO solutions are appearing to fill the security gaps of online business banking and cash management solutions, which were never intended as portal or SSO

solutions. The new integrated SSO combines user credential management for entity Websites with browser validation with a multi-layered security approach including strong authentication, software based keyboards to thwart keyloggers, one-time perishable pass-code generation and utilization, and strong authentication of destination Websites to prevent DNS poisoning and pharming.

The global economic costs of cyber crime are estimated at more than one trillion dollars and costs to the U.S. at about \$8 billion. The banking industry is moving to shared fraud analytics to detect cyber crime in flight, but it should also be prevented at the outset. Financial products with built-in security are absolutely essential. Industry groups, banks and technology companies are emerging to fill the gaps and build the online experience with the proper foundation to mitigate threats that have moved beyond network perimeters to applications and data.

*Joe Spatarella is vice president of sales and marketing for Online Banking Solutions.*

Posted with permissions from the January 25, 2010 issue of [Bank Systems & Technology](#), United Business Media LLC. Copyright 2010. All rights reserved.  
For more information about reprints from Bank Systems & Technology, contact [Wright's Reprints](#) at 877-652-5295.

## About Online Banking Solutions (OBS):

Founded in 2002 by a management team that pioneered Web cash management and business banking technology, launching two successful financial technology companies, Online Banking Solutions (OBS) provides next-generation Online Messenger multi-channel reporting, transaction and file delivery services to banks including seven of the top 50 U.S. financial institutions. Private, profitable and based on the philosophy of over servicing clients, OBS offers financial institutions the extensiveness of a large-scale technology provider, but the tenacity of an agile, service-driven organization. For more information, visit [www.onlinebankingsolutions.com](http://www.onlinebankingsolutions.com).

ONLINEBANKINGSOLUTIONS 

75 5TH STREET NW, SUITE 322, ATLANTA, GA 30308  
404-526-6055