BANK TECHNOLOGY NEWS
btn

PERSPECTIVE

ID-Theft Fears Keep Clients Off the Web

Bank Technology News | Tuesday, April 1, 2008

By Joe Sowerby

The electronic channel is broken.

Rather than flocking to this convenient channel for communications and transactions, bank customers are hesitating and, in many cases, taking a step back, concerned about their online security. Financial institutions are helplessly watching their most cost-effective, efficient channel fall by the wayside. A review of how the industry reached this sorry state — including connecting the dots between cause and effect—will help determine how to salvage the electronic channel and make it work for the customer and financial institution.

Anti-virus products have been available since the first viruses emerged on the Internet some 25 years ago. At that time, an ineffective process materialized whereby a new threat would emerge, and consumers would download a new product to address it. Although inconvenient for customers, this practice worked for a few years. Then, the landscape changed. Hackers, whose main goal had been to be disruptive, began to gain a measure of notoriety. These online con artists began to make significant money, $25,000 a day or more. Yet with no way to move or launder their ill-gotten gains, they developed relationships with organized crime, a group well-versed in money laundering and related illegal activities. In short order, organized crime noticed the big money available from illegal online activity and began hiring computer-science graduates from some of the best schools, offering annual salaries of $500,000 or more.

In an attempt to fight back, industry groups banded together. Their solution was to educate the consumer. Armed with rudimentary information, unsophisticated users did the best they could, which was to delete all unrecognized email. Given this understandable reaction, email was no longer a viable option for financial institutions to safely interact with customers.

More recently, Trojan, man-in-the-middle and browser-based attacks have emerged as major online threats. Again, the industry response is to educate the user, suggesting that customers visit supposedly secure bank Websites. In fact, criminals are waiting for consumers to rely on their browser to communicate and transact with their financial institution. Browsers are as secure as email for online financial services, which is to say not at all. As threats to the browser emerge and become public, users will revert to past behavior and stop connecting to bank Websites altogether.

At that point, what happens to banks' electronic-delivery strategy?

This is not an insignificant issue. Banks do not want to return to costly brick-and-mortar or call-center interactions with customers. It costs the institution about $4 every time a customer visits a branch, versus fractions of a penny online. Plus, financial institutions have spent millions of dollars on the online-delivery channel. They've built business processes around it, and a large and growing number of customers were adopting it because of its great convenience. The current state of affairs is a lose-lose proposition for both the customer and the financial institution.

In addition to loss of goodwill, there is a financial cost to institutions as well. To this point, banks have covered customer losses due to online identity fraud. Yet as online attacks proliferate, institutions will resist covering increasingly large customer losses. This state of affairs will lead to an inevitable showdown between customer and financial institution.

Smart consumers will attempt to avoid this scenario by setting up their bill payments on their credit cards, preferring to write a single check once a month. Yet, this course of action merely extends the burden to credit-card companies and merchants, whose customers will hold them accountable for covering losses when the inevitable online crimes occur.

Financial institutions will be standing by the tracks as the train wreck approaches, seemingly helpless.

If the industry's first solution was to educate the customer, the second is to deploy multi-factor security. With the discarding of emails and the imminent shutdown of browser connections, customers will now have to use another security factor. In theory, this approach appears promising. The criminal can not access the additional factor—and all is well. Actually, it's not. While criminals may not be able to retrieve a customer's funds, they can still access the customer's identity. Already, criminals are opening credit-card accounts and buying homes using someone else's identity. In addition to large legal fees and significant stress, it can take years to resolve ID-theft issues. This is the emerging new crime.

The reality is that customers will balk at a layered defense strategy. The expense and hassles may be prohibitive. To work optimally, this approach requires a Macintosh computer with the most recent security updates running Safari, anti-virus software, anti-spyware utilities, secure toolbars, with the entire setup running behind a firewall. Even with all of these layers, customers still won't be secure. Emerging Trojan threats like Rustoc. B and Gozi can circumvent many defense layers. New attacks can elude and switch off anti-virus defenses and the new class of DNS attacks effectively bypasses browser-based security indicators and defenses.

Customers like to bank online, and they will adopt a new approach that empowers them to do so. According to Pew Internet and American Life Project, adoption is increasing, but not nearly at the rate of broadband adoption. The main reason: fear of online identity fraud.

New and emerging threats require a new approach. An entirely new channel— designed to be secure and closed to online criminals—is the answer. By using this new approach, financial institutions will regain control of the electronic-delivery channel. Customers will enjoy its convenience. At the same time, banks will benefit from customers adopting the most cost-effective and efficient channel available. Connecting the dots in this manner adds up to a win-win for customers and financial institutions.

Joe Sowerby is CEO of Armored Online.