AMERICAN BANKER.

CRISIS CONTROL: TextPower has developed an "incredibly secure" system that turns traditional text-based authentication inside out, CEO Scott Goldman says; Vorstack sells security professionals software that helps them sort through their "5,000 emails a month" to identify the biggest threats, says Joe Eandi, CEO of Vorstack.

Data Breaches Spur Security Focus at Financial Startups

by Kevin Wack
MAY 2, 2014 3:43pm ET

Technology companies are debuting data-security products aimed at both banks and consumers in the

SAN JOSE, Calif. — The mounting threat of cyberattacks has spooked everyone from the biggest banks to average U.S. consumers.

At a financial technology conference in Silicon Valley this week, one major theme was how to enhance digital security inside of banks. Startups unveiled products designed to enable banks to share more information about cyberthreats, to authenticate customers in new ways and to combat fraud by allowing consumers to turn off their debit and credit cards.

What follows is a rundown of new data-security technology introduced at the Finovate conference.

Information Sharing. Two startups unveiled products that take advantage of "network effects" — a term that refers to services that become more valuable as more people use them — in an effort to combat cybercrime.

Chicago-based Rippleshot is selling cloud-based software that's designed to determine quickly when and where retail data breaches have occurred. As banks report fraudulent transactions to Rippleshot, the software works to determine what the breached cards have in common.

The goal is to pinpoint the source of the breach by combing for the one specific retail location where all of breached cards were used.

"So if we can detect it early, and find out all the cards that were compromised at the location, and tell banks to reissue them before they become fraudulent, then they save money," Rippleshot Chief Executive Canh Tran says. "The power grows as more data comes in."

Vorstack, in Los Altos, Calif., has built software designed to make it easier for banks to share information about attacks by hackers and other cyberthreats.

The software has two main capabilities, according to Vorstack CEO Joe Eandi. First, it standardizes disorganized information in

an effort to determine its relevance. That service becomes more valuable as more banks join.

Second, the software automates the process of sharing information about cyberthefts among security professionals, which saves time inside banks from day one, according to Vorstack.

"If you look at a typical security professional, they may get 5,000 emails a month," Eandi says. "And all of that information is in different structures and different formats, and it actually creates more work for them."

"We are this thin layer that allows for automation of collaboration," he adds.

Authenticating Users. Because the password is passé, lots of companies are competing to offer banks more secure ways to authenticate their customers' identities.

San Juan Capistrano, Calif.-based TextPower uses text messages to authenticate users, but in the reverse way from most existing technologies.

Rather than sending a text message to the customer's mobile phone, the company's TextKey system instructs the user to send a text message to a specified phone number. That latter method is more secure because of quirks in the design of the U.S. text-messaging system, according to TextPower CEO Scott Goldman.

"When you send a text message to a phone, there's no security at all," Goldman told the audience here Tuesday. "However, when a text message is sent from a phone, it's incredibly secure."

Until late last year, Norway-based Encap Security was focused on

selling its authentication technology in Europe, where credit-card issuers long ago switched to chip-and-pin cards.

Following that conversion, in-store card fraud in Europe fell substantially, but fraud involving Internet purchases increased, as scammers quickly learned that the chip-and-pin technology does not prevent online fraud.

Now that same conversion process is finally on the horizon here in the United States, and Encap is marketing an authentication process that U.S. banks can use to combat the fraudulent use of chip-and-pin cards to make online purchases, as part of a comprehensive approach to preventing fraud.

Turning Off Debit and Credit Cards. With consumers nervous in the wake of the high-profile data breaches at Target and elsewhere, two companies introduced new products designed to give shoppers more control.

San Jose-based Ondot Systems has developed software that allows consumers, through the use of a mobile app, to turn off their debit and credit cards. So shoppers can unlock a particular card shortly before they make a purchase, and then quickly lock it again.

"With a single touch on the phone, you can turn your card on or off," Ondot CEO Vaduvur Bharghavan says.

The technology can also be used to set specific controls on a debit or credit card, such as the geographic area where it can be used, or the types of stores where transactions will be accepted.

Ondot is marketing its technology to banks and credit unions, which can either incorporate it into their existing mobile banking apps, or sell it separately to their customers.

Palo Alto, Calif.-based Red Giant has developed similar

technology, but it is selling its product directly to consumers. Shoppers turn on their Red Giant cards to make a specific purchase, and the cards turn off automatically when they leave a designated geographic area surrounding that particular store.

"Most of the time it's locked, because most of the time it's sitting in your wallet, and you don't want anybody using it," Red Giant CEO Robert Sears explains.

The Red Giant card also includes a suite of financial management tools. The company plans to charge users a $4.95 monthly subscription fee, according to Sears.