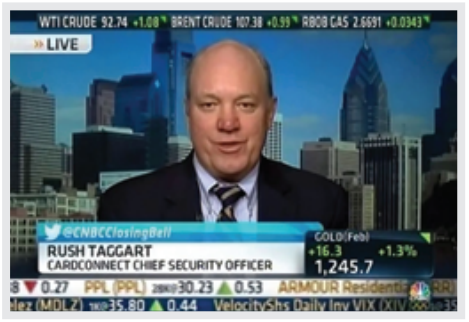
Payment Security Experts

As seen on...

"Chip and PIN would have not stopped the breach but the data stolen would have been much less useful. Today's mag-stripe technology in the United States is the equivalent of leaving the front door of your house wide open."

- CardConnect's Chief Security Officer Rush Taggart on CNBC's Closing Bell



THE WALL STREET JOURNAL.

"What ultimately is the answer for merchants is to minimize or eliminate the problem of PCI compliance. The tokenization of cardholder data goes a long way to doing that, and using compliance service providers will be a major aspect of it going out from 2014 into 2015. Aggressively migrating to chip-and-pin and a point-to-point encryption-compliant solution is the only way out for merchants."

- CSO Rush Taggart

"It used to be that you just had to evaluate malware threats against platforms that were common malware victims. Now, in PCI DSS 3.0, merchants must identify malware threats for all platforms, from tablets all the way up to their in-store swipe terminals. Had Target implemented this 3.0 step, it might have helped to better anticipate or detect the attack."

- CardConnect's Director of Technology Nick Aceto

USA TODAY
A GANNETT COMPANY

REUTERS

"There's no doubt in my mind increased card security will happen over the next two years. The fraud risk is too high. I think we all wish it had happened over the last four years."

- CSO Rush Taggart

"With constantly emerging threats carried out by increasingly intelligent hackers, companies should operate under the assumption that their data will be compromised at some point. What encryption and tokenization can do is soften the blow, should a breach occur; cyber thieves cannot decrypt or read stolen card data without a key, and tokens stored in a secure vault essentially are meaningless to anyone but the merchant and its payment processor."

- CardConnect's Director of Integration Services David Kilgallon

CSO
SECURITY AND RISK
