***Independent Banker***

**From the Top**

**October 2022**

[tag]

**From the Top**

[byline]

**Brad M. Bolton**

**Chairman, ICBA**

Brad M. Bolton is president and CEO of Community Spirit Bank in Red Bay, Ala.

When it comes to fraud, you don’t know what you don’t know, and what you don’t know can greatly influence your bottom line. But the effects of fraud are felt far beyond budgetary impact; our reputations are at risk. Customers expect their bank to keep their money safe, and though they most often are the gateway for fraud, they are inclined to blame us if we can’t fix the problem.

So, we are in a unique position as community bankers—between a rock and a hard place—trying to thwart attacks and keep the banking experience a positive one for our customers. We have to stay on top of emerging threats through continuous staff education and technology enhancements. Solutions like dual authentication and customer card controls can help in sidestepping some of the risk, and continuous cyber training for bank staff can help them remain vigilant against phishing emails and more.

Fortunately, this work arms us with fraud prevention expertise. While hard-earned, the knowledge we have cultivated over years of circumventing attacks means that we have a depth of understanding about cyber and data security that the general population doesn’t—and those are lessons we can share.

We, as community leaders, have an opportunity to provide value-added insights to our municipalities, small businesses, schools and beyond. If we share our experiences, advise employers to train their employees and offer greater information to consumers, we are taking our work one step further in helping to protect our communities.

These efforts don’t have to be new initiatives. Consider holding quarterly meetings with your small business customers: How can you incorporate some cyber and data security education into those sessions? Or think about your team’s roles on various boards and committees and how they can raise this topic as an agenda item. Or explore ways to introduce these concepts in school or public presentations. This type of education is important, and it’s something we all should be doing.

Because with cyber and data security, as with everything else in community banking, it all comes back to relationships. If our customers are unsure about an email or text message and they decide to call us before acting on it, that’s the first step in stopping the attack and a clear sign that sharing information is paying off. That’s the power of the relationship shining through and trumping anything the dark web can throw at us. When our customers know we will help protect them against fraud, they gain a peace of mind from that relationship that only we, as community banks, can provide.

[twitter]

Connect with Brad **@BradMBolton**

[sidebar]

My top three

**Cybersecurity tips for community banks**

1. Explore .bank and Sheltered Harbor for a more secure digital fingerprint.
2. Incorporate dual authentication for transaction-based processing.
3. Ensure your cyber insurance coverage matches the breadth and complexity of your business.

[pull quote]

“While hard-earned, the knowledge we have cultivated over years of circumventing attacks means that we have a depth of understanding about cyber and data security that the general population doesn’t—and those are lessons we can share.”