



Cyber Risk Month - Knowing The New Risks

cyber security

Summary: We bring you the latest updates on biometric privacy laws as you seek to strengthen your cybersecurity.

The Census Bureau reports about 13% of US adults have a master's, professional or doctoral degree. That shows there are plenty of smart people roaming around the country, so community bankers might want to brush up marketing efforts to find a way to capture them as customers.

On another matter, banks should also brush up on a growing number of state privacy laws pertaining to the use of fingerprints, iris scans and voice prints to authenticate employees or customers - because your bank could face significant lawsuits even for technical violations.

So states Chubb's latest Cyber InFocus Report, "[Know the Latest Trends in Cyber Risks](#)," which details some of the most pressing threats, particularly for banks.

IL was the first state to enact a law to safeguard fingerprints and other biometric identifiers. The 2008 passage of its Biometric Information Privacy Act (BIPA) requires notice before such information is collected, has rigorous consent requirements, limits the sale and disclosure of the information, requires reasonable care to safeguard biometric information, prohibits the retention of biometric information beyond the purpose for which it was collected, and requires that a private entity establish and maintain a retention policy that provides for the permanent destruction of biometric information when the initial purpose for collecting/obtaining it has been satisfied.

Other states have followed suit. TX and WA have biometric privacy laws in place, and CA's law becomes effective in 2020. These are followed closely by AZ, FL and MA, which have bills introduced in their legislatures while lawmakers in other states are considering the same.

The main difference between these BIPA laws is how states are choosing to enforce them. For example, while the TX law permits only the state's attorney general to enforce violations, IL allows private actions by individuals and class-action lawsuits.

Indeed, class-action plaintiffs in The Land of Lincoln can bring suit on the basis of a technical violation alone, and without the need to prove that they suffered actual damages--so ruled the IL Supreme Court last January on the landmark case *Rosenbach v. Six Flags*. Now more companies operating in IL are being named defendants in BIPA-related litigation.

Banks continue to be a prime target for cybercrime, so it is natural that better protections, such as biometrics would be in the discussion. The key here is to thoroughly research what you are thinking of rolling out and then carefully comparing it to your state of operation or perhaps even where your customers may reside (full or part-time).

A Pandora's box has opened, so bankers need to be extra vigilant and careful as you slowly move into the world of biometrics.

Since October is Cyber Risk Month, we thought it was a good time to think about how to mitigate the latest threats, as you seek to address the latest laws.

EXPAND INTERNATIONAL RISK CONSULTATION CAPABILITIES

Your bank can offer [foreign exchange forward contracts](#) that allow your customer to manage exchange rate risk while you generate extra fee income. Contact us today for more information.

Copyright 2021 PCBB. Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.