Trying to Put a Finger on the New Frontier of Privacy Compliance: Biometric Data

Indiana Bankers Association
December 8, 2017

Unlike social security numbers or credit cards, you can't change your retina or fingerprint. Perhaps for that simple reason, biometric data may be the new black in terms of security and employment procedures for companies of all shapes and sizes. Many employers now require employees to sign-in with a thumbprint, and banks have begun to utilize Thumbprint Signature Programs, a cutting-edge means by which a person can open a bank account or cash a check.

This trend toward using biometric identifying information, while rooted in the hopes of fraud protection and convenience, brings with it compliance concerns of serious note. Take, for example, Illinois. In 2008, the state enacted the Illinois Biometric Information Privacy Act ("BIPA"), in an effort to protect against theft of biometric data. Texas and Washington have followed suit, and other states have considered similar legislation, given the lobbying of privacy activists.

The laws require specific disclosure and destruction protocols. In Illinois, for instance, companies with biometric information must: (1) develop a written policy made available to the public; and (2) establish a retention schedule and guidelines for destroying the information. Employees and customers who provide biometric data need to provide a written release, and the companies can't sell or disclose that biometric data.

Failure to make appropriate disclosures regarding the collection and storage of biometric data—together with failure to ensure sufficient protections are in place to lessen the chances of a breach—can land a company in hot water. BIPA lawsuits are popping-up on a weekly, if not daily, basis and have eye-popping price tags because they are regularly brought as class actions with statutory damages ranging $1,000 to $5,000 *per violation*. Attorneys' fees and costs can be awarded.

Why all the hubbub? Currently, there is no remedy available if biometric data is stolen. Standard protections and protocols such as encryption don't apply to biometric data—you can't encode your body parts. And, then, if someone steals biometric information as found in a bank card, this biometric information can be used to obtain fraudulent biometric-based identification.

PROFESSIONALS

Molly A. Arranz
Partner

RELATED SERVICES

Banking & Finance

Cybersecurity & Data Privacy

Trying to Put a Finger on the New Frontier of Privacy Compliance: Biometric Data

This trend should fall on your radar. The Indiana Bankers Association recently adopted a Thumbprint Signature Program (something originally developed by the Texas Bankers Association which has spread to 38 endorsing state bankers associations). This program was meant to provide a simple, effective and inexpensive method for preventing and deterring check fraud.

Though the program has received much acclaim—participating institutions report a significant reduction in losses from fraudulent checks cashed—potential lawmaking over this collection of biometric data could pack a serious punch. Indeed, banks are high value targets for hackers, and failure to ensure proper protection for biometric data could compromise the identity of countless customers which can trigger a costly lawsuit and create a PR nightmare.

Companies would do well to audit their privacy policies and other written disclosures. Best business practices require a careful look into retention and cataloging of any biometric data—both in-house and by third-party providers. At this time, Indiana does not have biometric privacy legislation similar to, for example, Illinois; but, not having a specific statute or law in place will not dissuade customers, armed with creative legal counsel, from pursuing a privacy claim or cause of action.