FEATURED ARTICLE

THE (BANKING) WORLD AT YOUR FINGERTIPS: THE RAPID RISE OF FINGERPRINT BIOMETRICS IN THE BANKING INDUSTRY

David J. Oberly, *Data Privacy/Cybersecurity Attorney,* **Blank Rome**

Just a few years ago, the thought of being able to use your fingerprint to gain access to your bank account through your mobile phone seemed like pure science fiction. Fast forward to 2020, and fingerprint-based biometrics are now widely used by companies of all types, including those in the banking industry. At the same time, fingerprint biometrics carries with it sizeable security risks and challenges, which have prompted attempts by legislators across the U.S. to impose stringent requirements and limitations on its use.

Adding to the risks and challenges of this popular form of biometrics is the fact that fingerprint readers have become far and away the number one target for class action litigation brought under new stringent biometric privacy laws. Financial institutions utilizing fingerprint biometrics must be cognizant of the challenges, risks and potential legal liability posed by this technology and take proactive measures that both minimize risk and comply with the law.

Biometric Fingerprint Technology: How it Works

Biometric fingerprint technology involves the process of using 'biometrics' (i.e., individual physical characteristics) to scan a finger and identify its geometry by measuring length, width, thickness and surface area. These measurements are then converted into a mathematical algorithm known as a digital template and stored in a database. During this process, however, no actual fingerprint image is ever created. To identify or verify a fingerprint, an algorithm compares the new template created from the extracted data points of the fingerprint that has been placed on a biometric scanner with a previously-stored digital template. In total, the entire verification/authentication process takes approximately one second.

The Impact of Fingerprint Biometrics in Banking

Fingerprint biometric technology has become increasingly popular. It is now heavily relied upon in a range of different commercial contexts due to its ability to enhance the efficiency, effectiveness and security of business operations. Fingerprint biometrics has seen a rapid rise particularly in the banking industry for a number of reasons. One of the most significant reasons stems from the technology's ability to enhance **>>**

> *"The use of fingerprint biometrics, by contrast, completely eliminates the need for passwords to access accounts or devices. These enhancements in ease-of-use and efficiency have made fingerprint biometrics an extremely popular method of authentication for a wide variety of banking activities."*

the customer experience. Today, we use hundreds of passwords across our heavily connected lives, and remembering each one can be a challenging ask – one that causes businesses to lose out on millions of dollars of revenue per year. According to a recent MasterCard study, one in every three online transactions is abandoned due to consumers' inability to remember their passwords.

The use of fingerprint biometrics, by contrast, completely eliminates the need for passwords to access accounts or devices. These enhancements in ease-of-use and efficiency have made fingerprint biometrics an extremely popular method of authentication for a wide variety of banking activities. In this respect, according to a recent Visa study, customers are as likely to favor using fingerprint recognition technologies for in-store transactions as they are for mobile or online transactions. Of all the biometric authentication techniques currently available, fingerprint biometrics ranked the highest in terms of desired payment authentication.

In addition, fingerprint biometrics also provide a significantly enhanced level of security for banks compared to traditional passwords. Unlike passwords, fingerprint biometric technology authenticates customers according to who they are, as opposed to what they know. Thus, fingerprint recognition operates as a method of two-factor authentication in and of itself – first, with possession of the individual's device, and second, with his or her unique fingerprint characteristics. Consequently, fingerprint biometrics have become a main player in the banking industry's ongoing battle against fraud across multiple payment channels.

Enhancing Banking Operations and Boosting Revenue

Fingerprint biometrics are being used in a rapidly-increasing number of contexts within banking to enhance the efficiency, effectiveness and security of banking operations.

Its most common use is within mobile banking. According to a recent Juniper Research study, biometric authentication will be used to protect $2.5 trillion in mobile transactions by 2024, a tenfold increase compared to 2019. And according to a recent Goode Intelligence study, there will be over 2.6 billion biometric payment users by just 2023. Beyond mobile banking, fingerprint biometrics are also being commonly deployed in bricks-and-mortar branches and incorporated into ATM machines.

Fingerprint biometrics are also being leveraged by the banking industry to offer customers technologically-advanced biometric payment cards, which provide both significantly enhanced security and reduced transaction times compared to to traditional PIN numbers and signatures.

Security Challenges & Risks

However, Fingerprint biometric technology also carries fairly sizeable security challenges and risks.

The first pertains to security of stored fingerprint template data. Passwords can be easily changed if stolen; conversely, once fingerprint template data is compromised it has lost its ability to be used as a secure identifying feature. Compromised fingerprint template data also has significant security implications for users across multiple accounts and devices.

Second, fingerprint recognition technology on mobile devices offers a significantly lower level of security than dedicated fingerprint biometric systems. Indeed, mobile device fingerprint recognition utilizes only a partial fingerprint recognition algorithm.

Third, fingerprint biometric technology also presents a risk in relation to impersonation and spoofing, where fake fingerprints are used to foil biometric fingerprint readers. In one experiment, a 3D printer was used to create fake fingerprint molds that were cast onto materials such as silicon and fabric glue. This produced an 80% success rate in defeating fingerprint authentication systems. Similarly, Samsung recently experienced an incident whereby anyone could bypass the company's Galaxy S10 fingerprint sensor if a third-party silicon case was used to enclose the device.

The Legal Landscape

Due to concerns about companies using biometric fingerprints in a safe and responsible manner, lawmakers across the country have sought ways to stringently regulate this technology.

First, legislators have sought to add fingerprint template data to the types of protected personal information which, if compromised, triggers breach notification obligations by impacted entities.

Second, new state consumer laws – most notably the California Consumer Privacy Act (CCPA) – also include fingerprint template data (and other forms of biometric data) within their definitions of personal information and place a range of requirements and restrictions on the utilization of that data. While the CCPA provides an partial exemption for GLBA-regulated entities, financial institutions must comply with the CCPA when using fingerprint biometric data for purposes other than providing a financial service or product. Along the same lines, other states are taking a page out of California's playbook and have ramped up their efforts in 2020 to put in place their own copycat CCPA laws. **>>**

Third, to combat the risk that fingerprint template data and other biometric data poses, several states have enacted new laws that focus directly on regulating the collection and use of fingerprint template data by business entities.

Overall, Illinois's Biometric Information Privacy Act (BIPA) is generally considered the most stringent. BIPA contains a private right of action provision that permits the recovery of statutory damages ranging between $1,000 and $5,000 by any aggrieved person under the law. This has generated a tremendous amount of class litigation from consumers alleging mere technical violations of the law, including a $550 million settlement by Facebook to resolve recent BIPA litigation. With that said, BIPA provides a complete exemption for financial institutions and their affiliates that are subject to the GLBA.

Beyond Illinois, Texas and Washington have enacted biometric privacy laws that are similar, albeit less stringent, than BIPA. While Washington's law provides a complete exemption for GLBA-regulated entities, financial institutions are subject to the Texas law in connection with their use of fingerprint biometrics. Moreover, in addition to the laws currently on the books, states across the nation are also seeking to enact biometric privacy laws of their own, many of which – such as Idaho's HB 492 – provide no exemption for GLBA-regulated entities.

Finally, in addition to statutory law regulating the use of biometric fingerprint technology, companies also must be mindful of potential common law tort liability. In particular, tort claims for negligence and negligence per se may be pursued against banks and financial institutions that experience a breach event involving fingerprint data.

"Beyond Illinois, Texas and Washington have enacted biometric privacy laws that are similar, albeit less stringent, than BIPA. While Washington's law provides a complete exemption for GLBA-regulated entities, financial institutions are subject to the Texas law in connection with their use of fingerprint biometrics."

Best Practices to Minimize Liability Risk

Ultimately, there are many risks and concerns around the use of fingerprint biometrics that must be addressed. With data breaches increasing in frequency and severity, and the public's heightened concern regarding the threat of identity theft, banks and other institutions utilizing fingerprint template data must proceed with caution, even if they do not conduct business in locations where targeted biometric privacy laws are currently currently in place. Fortunately, there are several best practices that financial institutions can implement to minimize the risk of becoming embroiled in high-stakes class action litigation stemming from the use of fingerprint biometrics or other biometric data:

- as a starting point, ensure transparency by implementing a detailed fingerprint biometrics-specific privacy policy;
- to further support transparency, provide conspicuous, advance notice of the use of biometric fingerprint technology before any fingerprint template data is captured, used or stored;
- where feasible, obtain signed, written consent authorizing the collection, use and storage of fingerprint template data prior to the time any such data is captured or used for any purpose;
- implement effective data security safeguards to protect all data captured, used and stored through fingerprint biometric technology from improper disclosure, access or acquisition; and
- effectively manage risk and minimize liability in connection with vendors and other service providers by completing the necessary due diligence and vetting of all potential vendors, and ensuring that all vendor contracts directly address key biometric privacy issues.

Conclusion

Fingerprint biometrics are having an increasingly significant impact on every facet of the operations of banks and financial institutions. But this technology is not without its limitations and drawbacks. At the same time, states have also greatly increased their efforts in enacting new biometrics laws, many of which are modeled heavily after Illinois's stringent biometric statute. As such, entities operating in the banking industry that use fingerprint biometric technology should consider taking proactive steps to strategically enhance their biometric privacy compliance programs, while building in the necessary degree of flexibility to allow them to adapt to the foreseeable challenges associated with biometric privacy. ■

David J. Oberly is an attorney in the Cincinnati office of Blank Rome LLP and is a member of the firm's Cybersecurity & Data Privacy and Privacy Class Action Defense groups. David's practice encompasses both counseling and advising sophisticated clients on a wide range of cybersecurity, data privacy, and biometric privacy matters, as well as representing clients in the defense of privacy and biometric privacy class action litigation. He can be reached at doberly@blankrome.com.