Professional Perspective

Satisfying BIPA's Reasonable Security Requirement

David J. Oberly, Blank Rome

Bloomberg Law

Satisfying BIPA's Reasonable Security Requirement

Contributed by David J. Oberly, Blank Rome

The Illinois Biometric Information Privacy Act (BIPA) is, to date, the most onerous and expansive biometric privacy law in effect in the U.S. Notably, one of the most critical aspects of BIPA also remains one of the least discussed—data security. This can be attributed in large part to the fact that, to date, no high-profile BIPA litigation has centered on purported violations of BIPA's Section 15(e) data security requirements. This article provides a short overview of the current legal landscape, discusses the Section 15(e) data security requirements, and offers practical tips and best practices for compliance.

Legal Landscape

BIPA encompasses three core elements that require companies to maintain a publicly available privacy policy, including guidelines and schedules for the retention and destruction of biometric data; provide notice and obtain consent prior to the collection of biometric data; and maintain security measures to safeguard biometric data.

One of the most noteworthy aspects of BIPA is the law's private right of action, which allows for class action litigation and the recovery of between $1,000 to $5,000 in statutory damages for each violation of the law. These high statutory damages awards, combined with a very low bar for establishing liability, has led to a flood of bet-the-company litigation that has continued unabated for the last two years.

Companies that use biometrics must ensure they thoroughly address BIPA's security requirement as part of their comprehensive biometric privacy compliance efforts. Proactive measures can help shield from a potentially game-changing BIPA lawsuit stemming from a security incident involving biometric data. Prepared companies will also be able to point to their strong security measures as persuasive evidence that the company has satisfied the security requirements of Section 15(e).

BIPA's Section 15(e) Security Requirement

BIPA requires covered entities to implement and maintain data security safeguards to protect biometric data possessed and stored by covered entities from improper access, disclosure, or acquisition. Specifically, Section 15(e) of BIPA states:

> A private entity in possession of a biometric identifier or biometric information shall: (1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

BIPA provides no substantive discussion on how companies can satisfy the security component of the law that is set forth in Section 15(e). In particular, the law does not articulate any guidance of any kind for implementing security measures that would satisfy Section 15(e)'s requirement that companies use a reasonable standard of care to safeguard biometric data. As a result, significant uncertainty remains as to what businesses can do to meet the security component of BIPA compliance.

Compliance Checklist

Despite a lack of clear direction from the law, there are several practical, concrete steps that companies can implement to build a defensible biometric data security program. These steps should help a company withstand scrutiny in the event their biometric data security practices are challenged in court. By implementing the best practices described below, companies can position themselves to proactively minimize the risk of experiencing a catastrophic data breach involving biometric data. Further, they will be implementing robust security measures to aid in satisfying the reasonableness standard at the heart of BIPA's security requirement.

Reasonableness Standard

As a starting point, companies should remain cognizant of the fact that BIPA's security requirement does not provide for a strict liability standard. Rather, consumers will be required to establish that any data breach event resulted from the company's failure to implement and maintain reasonable security practices. The best practices discussed below will not ensure that companies are absolutely impervious to security incidents or claims asserted under BIPA Section 15(e). However, by incorporating the following protocols as part of a comprehensive data security program, businesses can provide themselves with the ability to establish that affirmative actions were taken to safeguard sensitive biometric data. This, in turn, will put them in the best position to successfully defeat any claims of inadequate security in violation of BIPA.

Implementation of Defensive Biometric Data Security Strategies

As data breaches will almost always trigger class action litigation under BIPA, companies should place a special emphasis on implementing defensive strategies to minimize the likelihood of a data breach occurring. Implementing stringent defensive security measures will allow businesses to demonstrate that proactive measures were implemented, along with robust security protocols that satisfy the reasonableness standard of BIPA Section 15(e) if the entity were to fall victim to a biometric data compromise incident.

Companies should consider implementing the following practices where feasible:

- Designate one or more employee(s) to manage and oversee the company's biometric security program.
- Implement a specified retention period and permanently dispose of stored biometric data once it is no longer necessary for the purpose for which the data was collected.
- Ensure that all biometric data is encrypted, both while at rest and in transit.
- Store all biometric data separately from other types of personal information such as names, birthdates, and account numbers.
- Maintain stringent password protection policies for all individuals who have internal access to the systems that collect and use biometric data or the location(s) where such data is stored, which should encompass elements such as password expiration, complexity, and length.
- Complete mandatory biometrics-focused cybersecurity awareness training for all employees on the company's security program and policies, as well as best practices for employees to follow to ensure both that biometric data is stored, handled, and transmitted safely, and that employees can identify and avoid attempted cyber-attacks targeting biometric data.
- Perform periodic risk assessments to identify the primary risks to the biometric data possessed and stored by the company and implement any necessary modifications to the entity's information security program to minimize these risks.
- Perform penetration testing on the company's networks and systems to identify any security vulnerabilities that could be exploited by hackers and implement any necessary modifications to the entity's information security program to minimize the risk of these vulnerabilities being exploited by malicious actors.
- Implement network security monitoring tools to identify and detect unauthorized access to biometric data, attempted cyber-attacks, and other malicious behavior.
- Utilize a strong firewall to protect the company's systems by controlling all Internet traffic that flows in and out of its networks, as well as antivirus protection, which can serve as the last line of defense should a malicious attack penetrate the perimeter of the company's network.

As the foregoing security protocols are commonplace and widely used by a broad swath of entities across a wide range of varying sectors, implementation of these security measures will also aid most entities in satisfying BIPA's requirement that its security measures comport with those commonly used within the private entity's industry.

Written Information Security Plan

Companies should also ensure that they formally document their biometric data security policies, procedures, and practices in a written information security plan. The WISP should entail a written record of all the various data security safeguards that a company has implemented that are appropriate to the nature of the biometric data that is possessed and maintained by the company.

In addition, the organizational WISP should also document the company's risk assessment and the safeguards that have been implemented to address and minimize those risks, as well as a detailed data breach incident response plan which addresses identified or foreseeable risks, and which can be rapidly deployed in the event the business experiences a breach of its systems or networks involving biometric data.

Vendor Due Diligence, Contract Considerations, & Monitoring

Companies must also ensure that their vendors and service providers also maintain the necessary security measures and protocols to safeguard the entity's sensitive data while in the hands of the vendor or service provider.

Cyber-attacks directed at vendors and service providers have spiked sharply in frequency, severity, and cost. Just one example is the data breach involving file sharing service vendor Accellion, which impacted many high-profile companies, including several Am Law 100 law firms and Fortune 50 companies. Weeks after the security incident was disclosed, some of these high-profile clients faced data breach class action litigation naming them as the target defendant as a direct result of their business relationship with the actual breach victim, Accellion.

As such, effective data security entails not only ensuring that a business's own networks and systems are secure, but also that sensitive data possessed or maintained by vendors and service providers is also adequately protected. This is especially important in the context of sensitive biometric data, as most biometrics systems require the use of multiple third-party vendors that are needed to supply the technology to process and store fingerprint biometrics, facial template data, and the like.

There are several practical steps companies can take to ensure their third-party vendors and service providers maintain the requisite practices and protocols. First, before entering into a relationship with any vendor that will have access to biometric data, necessary due diligence and vetting must be completed by the company's in-house lawyers—or, ideally, experienced outside biometric privacy counsel—to ensure the vendor's security measures are sufficiently robust.

The following are key due diligence areas that must be addressed when vetting any biometrics vendor:

- Implementation and maintenance of comprehensive, up-to-date security policies and incident response plans.
- Performance of regular penetration testing and security audits.
- Completion of background checks on all vendor employees and other individuals who will be given access to the company's biometric data.

Second, companies should also review and update their contracts with current vendors to take into consideration the principal issues raised by BIPA and other biometric privacy laws, including the risk of a breach event involving the entity's biometric data. In most instances, this task should also be carried out by experienced biometric privacy counsel.

The following are key contractual provisions that should be included in all agreements with biometrics vendors and service providers:

- Prohibition on the disclosure or sale of biometric data
- Compliance with laws
- Minimum data security standards
- Security incident standards, cooperation, and reimbursement of remediation expenses
- Audit rights

- Limitation of liability
- Indemnification

Lastly, companies must also ensure that their vendors and service providers continue to maintain sufficient security measures and data handling practices over time through ongoing monitoring.

All vendors and service providers should be reviewed periodically, such as through data security assessment questionnaires.

Those holding more sensitive data, or higher-risk vendors or service providers, should be subject to a more extensive review. For these high-risk vendors and service providers, the use of third-party audits should be strongly considered to ensure compliance with today's biometric privacy laws and industry best practices. Importantly, in doing so companies must have all audits conducted by experienced biometric privacy counsel to ensure that the audit is covered by the attorney-client privilege.

Conclusion

Today, businesses across all industries are experiencing more and more attempted—and often successful—data breach attacks from malicious outsiders, as well as data compromise incidents involving employees and other trusted insiders. Cyber-attacks and data breaches have become so commonplace today that it is no longer a matter of whether a business will fall victim to a data breach, but a question of when and to what extent a data breach event will take place.

At the same time, BIPA's vague security mandate, coupled with its expansive private right of action provision, greatly increases the potential scope of liability exposure faced by companies that handle biometric data and suffer a breach incident. As such, now more than ever, companies and their in-house counsel must take proactive measures and implement effective defensive mechanisms to shield their networks, systems, and devices from cyber-attacks targeting sensitive biometric data.