Articles + Publications | March 8, 2021

Taking Stock of Non-Monetary Settlement Provisions

Privacy & Cybersecurity Newsletter

WRITTEN BY

Hannah Oswald | P. Russell Perdew | Tara L. Trifon

Since the passage of the California Consumer Privacy Act and because of the continued interest in the Illinois Biometric Information Privacy Act, there has been a focus on the amount of money class members may expect to receive as part of a privacy or cyber class action settlements. But as the recently approved settlement in the Hanna Andersson, LLC data breach class action demonstrates, there is no one-size-fits-all agreement. Some settlements are purely monetary agreements that create a settlement fund for class members. Others focus on fixing particular issues or vulnerabilities and do not include any monetary relief. Some settlements have both monetary and non-monetary components. There are pros and cons to each type of agreement.

Even though monetary agreements may mean some money in the hands of an affected individual, the money is often insufficient to truly ameliorate the harm that a particular class member may have suffered. After all, unless an individual's misappropriated information was actually used for a fraudulent purpose or the plaintiff incurred out of pocket costs for services like credit monitoring, most class members can, at most, claim some undefined risk of future harm. Such a risk is vague, making it difficult to pin an appropriate price tag on compensation and potentially depressing recovery for class members who actually suffer harm. Further, such a settlement only benefits those that make such a claim in accordance with the approved procedures, so a class member who fails to do so will often receive no relief, though the settlement can nonetheless bar their claims.

To avoid these deficiencies, some privacy and cyber class actions have essentially functioned as private attorney general actions. The vast majority of settlements focus on the non-monetary settlement terms, or conduct remedy, in order to compel the defendant to fix whatever actually caused the issue. In some cases, the commitment to changing relevant business practices is the only substantive settlement term. Accordingly, conduct remedy provisions may be the most valuable part of the settlement, even though they may be difficult to quantify.

The Hanna Andersson Settlement

The recently approved settlement in the *Barnes v. Hanna Andersson, LLC*[i] is an example of the focus on non-monetary component of privacy and cyber class actions. Indeed, while the parties agreed to a modest settlement fund of $400,000, the more impactful terms involved the commitment to the business practice changes.

On February 3, 2020, Bernadette Barnes ("Barnes") filed a class action against the children's apparel company, Hanna Andersson, LLC ("Hanna"). Barnes alleged, among other things, that her personally identifiable information ("PII") was stolen as part of a data breach that occurred between September 16, 2019 and November 11, 2019.[ii] Barnes claimed the hackers obtained the information needed to illegally use the affected credit cards and that law enforcement officials found stolen names and card information for sale on the dark web.[iii] Hanna

customers were not notified of the breach until January 15, 2020 and Barnes filed her complaint shortly thereafter.[iv]

Four months later, the parties reached a settlement agreement that included a settlement fund of $400,000 (equal to approximately $2 per class member) in order to compensate class members, with an average expected payout of $38.[v] Importantly, the settlement also included broad business practice changes that Hanna is required to implement. For example, Hanna must conduct risk assessments consistent with the NIST Risk Management Framework, enable multi-factor authentication for all cloud services accounts, hire additional technical personnel and a director of cyber security (although not a chief information security officer), conduct phishing and penetration testing; and deploy additional intrusion detection and prevention, malware and anti-virus, and monitoring applications.[vi]

Barnes filed a motion for preliminary approval of the class settlement on November 19, 2020, arguing that the settlement was fair and reasonable.[vii] Specifically, Barnes claimed that the settlement achieved "an outstanding resolution" because class members would be able to recover their expenses.[viii] Barnes highlighted the corrective measures Hanna will be required to undertake in order to improve its cybersecurity, which changes will not only benefit the class members but "also other customers who make purchases from Hanna in the future."[ix]

On December 29, 2020, the Court preliminarily approved the settlement.[x]

What is the Value of the Non-Monetary Settlement Components?

Even though conduct remedy settlement provisions do not involve writing a check to a settlement fund, it is inaccurate to say that they do not involve an expenditure of money. For instance, with respect to the Hanna settlement, the company is now obligated to pay the salaries and benefits of the new personnel hires as well as the cost of the risk assessments, implementation of multi-factor authorization, and new software applications. As these are costs that the company will have to spend for the conceivable future, from the company's perspective, they have a real and quantifiable value.

From an individual's perspective, though, substantive business practice changes carry significantly more value inasmuch as they help reduce the risk of future issues. Money damages may help compensate those who have been affected by a privacy violation or cyber breach, but the actual amount that is disbursed to class members is usually modest. Additionally, it only compensates class members who actually submit claims, which is historically a small percentage of the potential claimants. On the other hand, conduct remedy helps all class members, regardless of whether they submit a claim, by reducing the likelihood that their PII will be misappropriated again in the future.

How impactful the non-monetary settlement terms may be depends on the degree of business practice changes that will be implemented. In some cases, a company only agrees to change its practices with respect to a single issue or program. For example, to resolve the class action asserting a claim under the Biometric Information Privacy Act,[xi] Facebook Inc. ("Facebook") only agreed to change the default settings that applied to the facial recognition product that was at issue. This simple change may not have an effect on the vast majority of Facebook users. But other settlements, like in *Hanna*, that require overarching conduct correction will almost certainly affect a much broader group of individuals.

Non-monetary settlement provisions may merely entail oversight to confirm that the company is indeed following its policies and procedures. For instance, Facebook suffered a cyberattack from July 2017 through September 2018 that affected 29 million users. Facebook then took steps to eliminate the vulnerability and increase its security measures after discovering the breach. Nonetheless, a class action was filed on September 28, 2018.[xii] After two years of litigation, the parties entered into a settlement agreement whereby Facebook would not have to pay class members any money (though it would pay plaintiffs' attorneys' fees of $16 million) and would also certify that the exploited vulnerability was terminated. Facebook also committed to certain security measures that would protect the personal information of all of Facebook users. But the court specifically noted that Facebook was voluntarily undertaking the security measures, and some of them were existing practices.[xiii] Given that the litigation apparently had little effect on Facebook's cybersecurity practices, the court stated that "th[e] external oversight becomes the real value for the class."[xiv]

Conclusion

Non-monetary settlement provisions can be a useful alternative where purely monetary provisions may not provide much compensation to class members. Non-monetary settlement provisions can also be a valuable addition to settlements with more notable compensation. How to value the non-monetary provision in a privacy and/or cyber class action settlement is highly dependent on the unique circumstances of every case. The real cost to the company of implementing the business practice changes (whether by purchasing additional software applications, conducting third party assessments, or hiring additional personnel) must be balanced with the less tangible benefit of mitigating future risks to the company and individuals. Regardless of the exact valuation, though, it is clear that non-monetary settlement provisions help ensure a more secure environment for the company and all the people whose PII was misappropriated. Thus, the focus on such terms in privacy and cyber class actions is likely to continue for the conceivable future.

This article first appeared in Law360 on February 9, 2021.

___

[i] See, Barnes v. Hanna Andersson, LLC, et al., Case No. 3:20-cv-00812-EMC.
[ii] Id, ECF No. 46.
[iii] Id.
[iv] Id.
[v] Id., ECF No. 59.
[vi] Id.
[vii] Id.
[viii] Id.
[ix] Id., Memorandum in support of the Motion for Preliminary Approval, p. 7.
[x] Id., ECF No. 68.
[xi] In re Facebook Biometric Information Privacy Litigation, No. 3:15-cv-03747 (N.D. Cal.).
[xii] See, Adkins v. Facebook, Inc., No. 3:18-cv-05982-WHA (N.D. Cal.).
[xiii] Id., ECF No. 314, p. 4.
[xiv] Id.

RELATED INDUSTRIES + PRACTICES

- Data + Privacy
- Privacy + Cyber