# LEGAL AND ECONOMIC ANALYSIS OF "RISK OF FUTURE ECONOMIC HARM" THEORIES **IN DATA BREACH LITIGATION**

**BY MIKE KHEYFETS**

**& GAVIN REINKE**

Mike Kheyfets is Partner in the Antitrust and Privacy & Data Security practices at Edgeworth Economics.
Gavin Reinke is a Partner at Alston & Bird who specializes in data privacy class action defense.

# TechREG CHRONICLE
# JULY 2026



Visit **www.competitionpolicyinternational.com** for access to these articles and more!

## LEGAL AND ECONOMIC ANALYSIS OF "RISK OF FUTURE ECONOMIC HARM" THEORIES IN DATA BREACH LITIGATION

By Mike Kheyfets & Gavin Reinke

This article examines one of the most contested areas of modern data breach litigation: claims based on an alleged risk of future economic harm. The authors assess both the legal foundations and the economic logic underlying theories that seek compensation for increased risks of identity theft, fraud, or other future injuries. Their analysis highlights significant challenges facing plaintiffs who attempt to transform speculative future risks into classwide damages claims, while also demonstrating the complexities involved in measuring economic harm arising from uncertainty itself.

In data breach litigation, plaintiffs often include allegations that they are facing an increased risk of future harm as a result of the data breach. In other words, plaintiffs allege that one way in which they have been harmed is that the exfiltration of data about them has increased the risk that, in the future, they will suffer some negative outcome (e.g., their identity may be stolen, their accounts may be hacked, they may become the victim of a phishing scam, etc.).

Traditionally, plaintiffs have relied on allegations of an increased risk of future harm, to varying degrees of success, to establish an injury-in-fact sufficient to incur Article III standing or to satisfy the damages element of their substantive claims. Courts acknowledge that "[e]vidence of a mere data breach does not, standing alone, satisfy the requirements of Article III standing."[2] But where a plaintiff plausibly alleges "an imminent and substantial risk of future misuse" of the plaintiff's personally identifiable information (or "PII"), based on the specific factual allegations made in the complaint, that can satisfy Article III's injury-in-fact requirement, "at least as to injunctive relief."[3]

In recent cases, plaintiffs whose allegations of a sufficiently imminent and substantial risk of future harm advanced beyond a motion to dismiss have attempted to rely heavily on those allegations to support their motions for class certification. They argue that these allegations can support a classwide damages theory that all individuals whose personal information was allegedly involved in the data breach at issue are now facing an increased risk of future harm and should be provided with compensation in the amount of the cost of purchasing commercial identity protection products well into the future to guard against that risk. This damages theory has been offered by Plaintiffs in several large data breach class actions, including a recent case filed against Accellion.

Though this damages theory is becoming more prevalent, there is very little case law substantively addressing it, as Courts have not had to squarely confront it for several reasons. For example, the Court in the *Accellion* case concluded that the Plaintiffs' expert was not qualified to offer certain opinions that were required to support this theory, and therefore did not consider this theory on the merits in ruling on the plaintiffs' motion for class certification.

In fact, there is only one court that has squarely addressed the merits of this damages theory. In *Adkins v. Facebook, Inc.*, plaintiffs sought certification of a negligence claim seeking, among other things, "for Facebook to provide cash for future credit monitoring" to the putative class members.[4] The court denied the plaintiffs' request to certify a class for damages. The court first held that the sole remaining plaintiff "has sufficiently established Article III standing because of a substantial risk of identity theft and also because he has lost time due to the breach."[5] Nevertheless, the Court held that the plaintiff could not "seek[] the cost of credit monitoring on behalf of the class" because "no decision supports that plaintiff . . . can allege a viable negligence claim under a credit monitoring theory," as plaintiff had not incurred any out-of-pocket expenses to purchase credit monitoring and because his alleged risk of future harm "does not rise to the level of appreciable harm to assert a negligence claim."[6]

This theory faces other legal challenges, too. In *Transunion LLC v. Ramirez*, the United States Supreme Court held that "the mere risk of future harm, without more, cannot qualify as a concrete harm in a suit for damages."[7] Allowing plaintiffs to recover monetary damages because of an increased risk of future harm would be inconsistent with *Transunion*. Under that Supreme Court precedent, to have Article III standing to sue for damages, a plaintiff must show that "exposure to the risk of future harm itself causes a *separate* concrete harm."[8]

***"In recent cases, plaintiffs whose allegations of a sufficiently imminent and substantial risk of future harm advanced beyond a motion to dismiss have attempted to rely heavily on those allegations to support their motions for class certification***

2 *Tsao v. Captiva MVP Restaurant Partners, LLC*, 986 F.3d 1332, 1344 (11th Cir. 2021).

3 *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 375-76 (1st Cir. 2023).

4 424 F. Supp. 3d 686, 690 (N.D. Cal. 2019).

5 *Ibid.* at 691.

6 *Ibid.* at 695-96.

7 594 U.S.413, 436 (2021).

8 *Ibid.*

At the motion to dismiss stage, plaintiffs typically couple their allegations about an increased risk of future harm with present allegations of injury, like time and money spent to monitor financial accounts or allegations of fraudulent charges on accounts. But even if a court finds those allegations sufficient to allow an individual named plaintiff to establish standing to sue for damages at the motion to dismiss stage, they are incapable of proof with common evidence and therefore cannot help plaintiffs carry their burden at class certification. Indeed, when plaintiffs attempt to rely on a class-wide damages theory predicated on an alleged risk of future harm, they often ignore the present injuries the named plaintiffs allege they experienced. Courts are likely to reject a theory that purports to allow putative class members to recover monetary damages as a result of an increased risk of future harm alone, as accepting that theory would violate *Transunion*. Thus, plaintiffs attempting to pursue this damages theory will face legal headwinds. Additionally, as discussed below, the theory — as it has been alleged in recent cases — is also not economically sound.

# 01

# PRINCIPLES OF ECONOMIC IMPACT FROM "RISK"

The term "economic impact" refers to whether a defendant's allegedly illegal conduct caused the plaintiff to be economically worse off. That is, a plaintiff is said to be "impacted" if their economic position in the actual world is worse than it would have been in a world where the alleged conduct did not occur (i.e., the "but-for world"). "Economic damages" refers to the magnitude of the difference between the two states of the world. In general, the exercise of determining economic impact and damages involves isolating and measuring the plaintiff's economic loss *caused* by the alleged conduct.

To illustrate a basic conception of measuring economic effects of "risk," consider the example of fraudulent withdrawals from a bank account. Risk of future loss from a fraudulent withdrawal may be conceptualized as the product of two factors: (i) the likelihood of such a withdrawal occurring, and (ii) the amount of the withdrawal if it were to occur. For example, if an individual faces a 1 percent chance of having $10,000 fraudulently withdrawn from their account, their risk of future loss of $100 (i.e., $10,000 times 0.01). If another individual faces a 0.1 percent chance of a $1,000 fraudulent withdrawal, that individual's risk of future loss of $1 (i.e., $1,000 times 0.001).

# 02

# WHAT "RISKS" ARE ALLEGED AS HAVING BEEN CAUSED BY THE CYBERATTACK?

When assessing potential economic impact in the form of "risk," it is important to articulate what negative outcomes the cyberattack at issue may cause plaintiffs, and how those translate into economic harm. For example, exfiltration of certain sensitive PII may in some circumstances potentially result in a risk of identity theft — which in turn may potentially result in the risk of economic loss from fraudulent bank account withdrawals, applications for loans or credit cards, or tax refunds. Alternatively, exfiltration of contact information may in some circumstances potentially result in an increased risk of unwanted calls and emails — a different type of negative outcome — which itself may potentially result in an increased risk of targeted scam and phishing attempts, in turn increasing the risk of financial loss from such scams.

Importantly, the types of even potential negative outcomes depend on a number of factors, including the particular types of information at issue — as do the risks of those outcomes being realized, and the associated potential economic loss. In fact, available research indicates that most data breach victims *do not* become victims of identity fraud — and of those that do, many do not suffer out-of-pocket financial losses.[9]

Even in a single cyberattack, different individuals may have different types of information accessed. For example, a single attack on a company may result in threat actors accessing (i) an employee's sensitive PII, (ii) a vendor's contact information, and/or (iii) a customer's username and login credentials. However, the potential negative outcomes that a threat actor could achieve with these different types of data would not be the same, and thus the risks to different kinds of data subjects would vary. For example, a vendor who has its contact information accessed — which may already be available in the public domain anyway — would not expose that vendor to a risk

9 "2014 LexisNexis True Cost of Fraud Study," LexisNexis, August 2014, Figure 7; Ericka Harrell and Alexandra Thompson, "Victims of Identity Theft, 2021," U.S. Department of Justice Bureau of Justice Statistics, October 2023, https://bjs.ojp.gov/document/vit21.pdf, Table 6.

of various types of financial fraud that require sensitive PII.

The nature of "risks" may even vary across ostensibly similar data subjects. For example, a company may retain more (and more sensitive) information about current employees than about terminated ones. Thus, a current employee that had his or her sensitive PII accessed may be differently situated in terms of exposure to risk than a former employee for whom the former employer retained only basic contact information. Put differently, the current employee in this example would be exposed to different *types* of risks, as well as to a different *likelihood* of negative outcomes actualizing, than the terminated employee.

# 03

# HOW DO INDIVIDUALIZED FACTORS AFFECT RISKS AN INDIVIDUAL FACES?

The nature of the information exfiltrated in a cyberattack is one factor that may differentiate individuals in terms of their risk exposure. (In fact, whether a particular piece of information was *exfiltrated* — i.e., was taken from the cyberattack target's network — or simply *accessed*, but not exfiltrated, can also result in differential risks.) However, other factors affecting risk of future loss could also vary across individuals. For example — as to the risk of economic losses associated with identity theft — some individuals may use security features like two-factor authentication and credit freezes, among others, that make unauthorized access to their assets less likely. Individuals that do not use the same types of security features may face higher risk of unauthorized access and economic loss. Additionally, the magnitude of unauthorized withdrawals (if they were to occur) may be limited by the amount of money in a specific account — or withdrawal limits placed on that account.

Similar issues arise for other types of information. For example, an individual that voluntarily posts PII on social media may have a different risk profile as compared to an individual that does not. An individual's PII may also be bought, sold, collected, and published by data aggregator companies — or subject to one or more other cyberattacks — and thus already outside the individual's ability to control its dissemination. That is, any individual's risk of any particular outcome is likely to depend on a variety of factors that are not specific to any single cyberattack.

The "vintage" of the information at issue may also be relevant to assessing an individual's risk of any particular negative outcome. Certain types of information (like contact information, insurance information, payment card numbers, and login credentials) can change, thus potentially changing the risk profile associated with their exposure because outdated information presents a different "risk" to the individual than current information. All these factors complicate (and individualize) the determination of that individual's "risk" from any particular cyber-incident.

> ***The nature of the information exfiltrated in a cyberattack is one factor that may differentiate individuals in terms of their risk exposure***

# 04

# CYBERATTACKS AND COMMERCIALLY AVAILABLE IDENTITY PROTECTION PRODUCTS

It is often the case that as part of notifying individuals that their data has been subject to a cyberattack, organizations also provide a no-cost offer of an identity protection product for a set period of time.[10] In some states, this action is compulsory in certain circumstances under state data breach notification laws[11] — while in others, it is done as a matter of standard business practice.

In practice, ex-post forensic assessment of a cyber incident may not precisely determine what information (if any) about a particular individual was subject to the attack. As a result, an organization may take the precautionary measure of notifying and providing no-cost identity protection products to an over-inclusive set of individuals. (For example, notification letters often emphasize that the recipient's information only *may* have been subject to the cyberattack.[12]) This means that some individuals whose information was not in fact accessed or exfiltrated may still receive an offer to enroll in the identity protection product.

Notably, even when offered identity protection products at no cost, many consumers do not accept them. For example, research has consistently found that many consumers do not enroll in identity protection products offered by the breached organizations — with reasons for declining the offer including (among others) lack of perceived necessity for these products or already being enrolled in a comparable product.[13]

The same identity protection products offered by breached organizations to consumers are also commercially available and can be purchased independently of an individual having been involved in a specific cyberattack. Increasingly, as referenced above, plaintiffs in data breach class actions seek to use the commercial availability of these products as a "proxy" for economic impact and damages in class action litigation.

***Notably, even when offered identity protection products at no cost, many consumers do not accept them***

10 See e.g., databases of data breach notification letters published by state authorities in California and Massachusetts.

11 See e.g., Cal. Civ. Code § 1798.82(d)(2)(G); Conn. Gen. Stat. § 36a-701b(b)(2)(B); 6 Del. C. § 12B-102(e); D.C. Code § 28-3852b; Mass. Gen Laws 93H § 3A(a); 73 Pa. Stat. § 2305d(a)(2); R.I. Gen. Laws § 11-49.3-4(e).

12 See e.g., databases of data breach notification letters published by state authorities in California and Massachusetts.

13 "The Aftermath of a Data Breach: Consumer Sentiment," Ponemon Institute, April 2014, , p. 5, Figure 6; Lillian Ablon, et al., "Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information," RAND Corporation, 2016, pp. 22–26, Figure 2.4; Peter Mayer, et al., "Awareness, Intention, (In)Action: Individuals' Reactions to Data Breaches." *ACM Transactions on Computer-Human Interaction*, vol. 30, no. 5, Sept. 2023, pp. 3, 16.

# 05

# ARE PRICES OF COMMERCIALLY AVAILABLE IDENTITY PROTECTION PRODUCTS A RELIABLE MODEL OF "ECONOMIC IMPACT DUE TO RISK"?

The assessment of how (if at all) a particular cyberattack caused any individual economic impact in the form of "risk of future harm" involves developing an economic model capable of measuring the *incremental* amount of risk of any particular outcome that was *caused* by the particular cyberattack at issue. A world where an individual faces *no risk* but for a specific cyberattack would not be appropriate, since in an appropriately constructed but-for world, the individual may still post information about themselves on social media, have their information bought and sold by data aggregators, and/or be subject to other cyberattacks or fraud. Put differently, the relevant question about economic impact from Cyberattack X is: "what risks would an individual face if Cyberattack X did not happen, but the world otherwise remained the same — including still posting on social media, still being subject to Cyberattacks Y and Z, still using the same data privacy practices, and so on?"

As the "risk of future harm" theories have evolved, litigants have sought to use prices of commercially available identity protection products as an "indirect" approach for assessing damages supposedly due to individuals from elevated risk. Although the articulation of the theory varies from case to case, the general reasoning that has been offered is that these products serve as mitigation of (or "insurance" against) certain cyber-risks and therefore the value of that risk can be approximated using their commercial value (i.e., prices).

As an illustration, consider a hypothetical identity protection product commercially priced at $99.99 per year. This product includes, among other features, (i) 3-bureau credit report and "dark web" monitoring, (ii) an identity theft insurance policy, (iii) fraud remediation and resolution, as well as (iv) credit lock. In the context of assessing economic impact and damages, a litigant may claim that the annual price of this product represents a proxy of the "risk of future harm" caused to them by a particular cyberattack. However, prices charged for these types of products differ from measures of "risk" attributable to a given cyberattack in several fundamental and important ways.

First, and most crucially, commercial pricing of identity protection products is determined by commercial factors that have no relationship to any alleged increase in "risk" for any individual related to any specific cyberattack. For example, if both an individual who was subject to Cyberattack X and one who was not can purchase the same product for $99.99, then that price does *not* reflect an increase in any particular "risk" specifically attributable to Cyberattack X.

As discussed above, the risk of a particular negative outcome caused by a particular cyberattack (if any) is a complex function of multiple factors. Some of these factors are cyberattack-specific (e.g., what information about the individual is at issue, whether it was only accessed or actually exfiltrated). Others are not (e.g., the individual's day-to-day data privacy practices, the availability of that individual's information in the public domain). A uniform price — such as the $99.99 in the above hypothetical — does not take into account any of these factors. It does not distinguish the individual whose sensitive PII was exfiltrated (potentially elevating their risk of becoming a victim of financial fraud) from the individual whose publicly available contact information was accessed in the cyberattack, posing no additional risk of such fraud.

Similarly, the uniform commercial pricing of an identity protection product cannot distinguish the risks (if any) to individuals who use security features like two-factor authentication, credit freezes, and account withdrawal limits from individuals that do not use these security features. Ultimately, these prices do not reflect (i) the likelihood of any particular negative outcome happening to any individual, or (ii) the amount of economic loss to the individual if any such negative outcome were to occur. The mismatch between the nature of risk (which varies with an individual's specific circumstances) and commercial pricing of an identity protection product (which does not) means that the latter would not be a reliable proxy for the former.

Second, commercial identity protection products are generally comprised of a broad range of features that may or may not be relevant to a particular cyberattack. For example, in addition to the features described above, suppose the hypothetical $99.99 per year product also includes antivirus protection, registered sex offender reporting, and a "vault" for storing passwords and sensitive digital files. Depending on the nature of a particular cyberattack with respect to an individual's information, these features may have no relevance to any "risk" created by the cyberattack — yet their value would be incorporated into the price charged by the provider. This would further detach the price of the product from the risk specifically *caused* by a particular cyber-incident.

Third, to the extent commercial pricing of an identity protection product is intended to proxy for an individual's willingness to pay for the mitigation of risks caused by a particular cyberattack, it is not clear that — absent evidence of an individual *actually engaging in such a transaction* — this is what that price represents. For example, the organization subject to the cyberattack may provide individuals with an identity protection product at no cost to them — and those individuals may or may not accept this offering (despite it costing them nothing). If an individual accepts the free offer, they may no longer need to spend $99.99 (or any amount) on additional products. If they do not accept the offer, there would be no reason to expect that they would be willing to pay $99.99 (or any amount) for something they did not accept at no cost.

Individuals may also be subscribed to one or more such products because they purchased them independently, were provided them as a result of having been in another cyberattack, or because they received those products as part of a transaction with a financial institution or another vendor. Thus, to the extent individuals already used (one or multiple) products that have (some or all) of the same featured included in the "proxy" product, the types of risks the proxy product would be intended for would already be monitored and the individual would not be willing to pay $99.99 per year (or potentially any amount) for a product that would be redundant.

In sum, for multiple reasons, using prices of commercially available credit monitoring products does not reliably measure the economic impact of an alleged increased risk of future harm following a cyberattack.

***"For example, the organization subject to the cyberattack may provide individuals with an identity protection product at no cost to them — and those individuals may or may not accept this offering (despite it costing them nothing)***

# CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.



CPI COMPETITION POLICY® INTERNATIONAL