EDITOR’S NOTE: CYBERVIOLENCE
Victoria Prussen Spears

CYBERVIOLENCE: THE THREATENING COMMUNICATION CASES
Ioana Vasiu and Lucian Vasiu

ROSENBACK v. SIX FLAGS AND EMERGING BIOMETRIC LAWS
Aravind Swaminathan, David T. Cohen, Rochelle Swartz, and Nicholas Farnsworth

FOURTH CIRCUIT SETS MIDDLE-OF-THE-ROAD THRESHOLD FOR ESTABLISHING ARTICLE III STANDING IN DATA BREACH CLASS ACTION LITIGATION
David J. Oberly

IN OR OUT? EDPB PUBLISHES MUCH-AWAITED GUIDANCE ON GDPR’S TERRITORIAL SCOPE
Huw Beverley-Smith, Jonathon A. Gunn, and Hans-Christian Mehrens

COMPLYING WITH A DATA SUBJECT ACCESS REQUEST: WHAT DATA CONTROLLERS NEED TO KNOW
Charles Wynn-Evans, Jennifer McGrandle, Emma Byford, and Rebecca Turner
<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Editor’s Note: Cyberviolence</td>
<td>Victoria Prussen Spears</td>
<td>105</td>
</tr>
<tr>
<td>Cyberviolence: The Threatening Communication Cases</td>
<td>Ioana Vasiu and Lucian Vasiu</td>
<td>107</td>
</tr>
<tr>
<td>Rosenbach v. Six Flags and Emerging Biometric Laws</td>
<td>Aravind Swaminathan, David T. Cohen, Rochelle Swartz, and Nicholas Farnsworth</td>
<td>116</td>
</tr>
<tr>
<td>Fourth Circuit Sets Middle-of-the-Road Threshold for Establishing Article III Standing in Data Breach Class Action Litigation</td>
<td>David J. Oberly</td>
<td>121</td>
</tr>
<tr>
<td>In or Out? EDPB Publishes Much-Awaited Guidance on GDPR’s Territorial Scope</td>
<td>Huw Beverley-Smith, Jonathon A. Gunn, and Hans-Christian Mehrens</td>
<td>125</td>
</tr>
<tr>
<td>Complying With a Data Subject Access Request: What Data Controllers Need To Know</td>
<td>Charles Wynn-Evans, Jennifer McGrandle, Emma Byford, and Rebecca Turner</td>
<td>131</td>
</tr>
</tbody>
</table>
Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF
STEVEN A. MEYEROWITZ
President, Meyerowitz Communications Inc.

EDITOR
VICTORIA PRUSSEN SPEARS
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

EMILIO W. CIVIDANES
Partner, Venable LLP

CHRISTOPHER G. Cwalina
Partner, Holland & Knight LLP

RICHARD D. HARRIS
Partner, Day Pitney LLP

JAY D. KENIGSBERG
Senior Counsel, Rivkin Radler LLP

DAVID C. LASHWAY
Partner, Baker & McKenzie LLP

CRAIG A. NEWMAN
Partner, Patterson Belknap Webb & Tyler LLP

ALAN CHARLES RAUL
Partner, Sidley Austin LLP

RANDI SINGER
Partner, Weil, Gotshal & Manges LLP

JOHN P. TOMASZEWSKI
Senior Counsel, Seyfarth Shaw LLP

TODD G. VARE
Partner, Barnes & Thornburg LLP

THOMAS F. ZYCH
Partner, Thompson Hine
Fourth Circuit Sets Middle-of-the-Road Threshold for Establishing Article III Standing in Data Breach Class Action Litigation

By David J. Oberly*

Today, a clear divergence of opinions exists among the federal courts of appeal as to the appropriate evidentiary threshold that must be met for establishing Article III standing, which varies significantly among the different appellate circuits. The author of this article discusses a U.S. Court of Appeals for the Fourth Circuit decision on the issue.

Adidas. Saks Fifth Avenue. Macy’s. Aside from being some of the world’s largest corporate entities, these companies are just a few of the more noteworthy businesses that have fallen victim to data breach incidents in 2018. At the same time that data breaches continue to increase in both frequency and severity, so too are lawsuits filed by those individuals whose data has been compromised as a result of these breaches. Today, a clear divergence of opinions exists among the federal courts of appeal as to the appropriate evidentiary threshold that must be met for establishing Article III standing, which varies significantly among the different appellate circuits. In *Hutton v. National Board of Examiners in Optometry, Inc.*,† the U.S. Court of Appeals for the Fourth Circuit just recently weighed in on this hot-button issue, holding that the theft of individuals’ personal identifying information (“PII”), combined with actual misuse of that PII, is sufficient to constitute a cognizable “injury-in-fact” for purposes of Article III standing, even where such misuse does not result in any pecuniary loss. In doing so, the *Hutton* court has paved a middle-of-the-road approach to the injury-in-fact prong of the standing analysis, further deepening the divide among federal circuit courts regarding the level of proof that is required to establish Article III standing in the context of data breach class action litigation.

FACTUAL & PROCEDURAL BACKGROUND

In July 2016, three optometrists and members of the National Board of Examiners in Optometry (“NBEO”) noticed that Chase Amazon Visa Mastercard accounts had been fraudulently opened in their names, which required use of their correct social security number and data of birth. Although the NBEO denied that their systems had ever been compromised, the optometrists determined that the only common source of

---

* David J. Oberly (doberly@blankrome.com) is an associate at Blank Rome LLP concentrating his practice in the areas of cybersecurity and data privacy, energy, environmental, toxic torts and mass torts, and product liability.
† No. 17-1506 (4th Cir. June 12, 2018).
their personal information was the NBEO. As such, the three optometrists filed suit, asserting several claims arising from the NBEO’s failure to adequately safeguard their personal information. The district court dismissed the optometrists’ lawsuit based on their failure to establish the injury-in-fact and traceability elements of the Article III standing analysis. The optometrists appealed.

**THE FOURTH CIRCUIT DECISION**

On appeal, the Fourth Circuit was tasked with resolving the question of whether the plaintiffs had pled sufficient facts to clear the Article III standing hurdle. The court answered that question in the affirmative, holding that the plaintiffs alleged a sufficiently concrete injury that was traceable to NBEO’s conduct which, together, was adequate to confer standing.

In its opinion, the court first assessed the injury-in-fact question. To establish an injury-in-fact, a plaintiff must show that he or she “suffered ‘an invasion of a legally protected interest’ that is ‘concrete and particularized’ and ‘actual or imminent, not conjectural or hypothetical.’” Applied to the optometrists’ claims, the court held that the theft of their personal information, combined with the subsequent misuse of this information in the form of identity theft and credit card fraud, constituted a sufficiently concrete injury to satisfy the injury-in-fact prong of the Article III standing analysis. Importantly, the court reached this conclusion despite the absence of any pecuniary loss in the form of fraudulent charges on their unsolicited credit cards, reasoning that settled U.S. Supreme Court precedent makes clear that the injury-in-fact issue is not confined to those who can show economic harm. In addition, the court further held that the out-of-pocket expenses pertaining to the purchase of credit card monitoring services incurred by the plaintiffs also represented a sufficiently concrete injury-in-fact to confer standing as well.

After disposing of the injury-in-fact issue, the court then assessed the traceability question. To establish this prong of Article III standing, the injury must be fairly traceable to the challenged action of the defendant. Applied to the optometrists’ claims, the *Hutton* court found that the plaintiffs’ allegations that the NBEO was the only common source that collected and continued to store social security numbers and (albeit outdated) personal information that was required to open the credit cards in the optometrists’ names was adequate to demonstrate that it was both plausible and likely that a breach of the NBEO’s database resulted in the fraudulent use of the plaintiffs’ personal information and the opening of the unsolicited credit cards, which in turn was sufficient to satisfy the traceability element of the Article III standing analysis.

Taken together, the Fourth Circuit concluded that the plaintiffs had set forth sufficient allegations to establish Article III standing at the pleading stage, thus requiring the reversal of the district court’s dismissal of the optometrists’ lawsuit.
TAKEAWAYS

There is a significant split among the federal appellate courts regarding what constitutes a sufficient injury-in-fact to confer Article III standing in data breach class action litigation. On one end of the spectrum, several courts of appeal – including the U.S. Courts of Appeals for the Second, Third, and Eighth Circuits – have followed the U.S. Supreme Court’s decision in *Clapper v. Amnesty International USA*,\(^2\) to require a data breach plaintiff to suffer actual harm, such as financial loss, in order to establish a cognizable injury-in-fact to confer standing. On the other end of the spectrum, several other appellate courts – including the U.S. Courts of Appeals for the Sixth, Seventh, and Ninth Circuits – have required only the existence of an increased “risk of future harm” to satisfy the injury-in-fact element of the standing test.

In *Hutton*, the Fourth Circuit has carved out a middle-of-the-road approach to data breach standing, taking the position that the combination of actual theft and subsequent misuse of PII is sufficient to constitute a cognizable injury-in-fact, even where such misuse does not result in any economic loss. In doing so, *Hutton* ultimately lowers the threshold for standing somewhat by not requiring any pecuniary loss to accompany the misuse of plaintiffs’ personal information in order to meet the injury-in-fact threshold for standing, thus continuing the trend by federal courts in lowering the threshold for demonstrating an adequate injury-in-fact in class action data breach litigation.

Importantly, the *Hutton* opinion provides valuable insight into the applicable evidentiary threshold for establishing a cognizable Article III injury-in-fact in data breach class action litigation, as much can be gleaned from comparing the *Hutton* decision with the Fourth Circuit’s recent opinion in *Beck v. McDonald*.\(^3\) In *Beck*, the court found that the plaintiffs lacked standing because they only alleged a “threat of future injury” where the theft of laptops and boxes containing personal information occurred, but the plaintiffs’ PII had not been misused. In doing so, the *Beck* court emphasized that a mere compromise of personal information and the resulting increased risk of future identity theft, without more, failed to satisfy the injury-in-fact element in the absence of identity theft or other misuse. Conversely, in *Hutton* the plaintiffs were found to have already suffered actual harm through the misuse of their PII, which was evidenced through the opening of unauthorized credit cards in the plaintiffs’ names. As such, *Hutton* demonstrates that the targeted theft of individuals’ PII, combined with actual misuse of that information, will generally be sufficient to clear the injury-in-fact hurdle for purposes of the Article III standing, even where such misuse does not result in any pecuniary or economic damage.

In addition, *Hutton* is also illustrative of the threshold that must be met for claimed injuries in the form of costs incurred for mitigating measures to safeguard against

\(^2\) 133 S.Ct. 1138 (2013).
\(^3\) 848 F.3d 262 (4th Cir. 2017).
future identity theft. In *Beck* the court held that this type of alleged injuries fell short of constituting a cognizable injury-in-fact because they were “self-imposed harms” that were incurred in response to a “speculative threat,” i.e., their fear of future harm, where they were not accompanied by any actual misuse of the plaintiffs’ personal information. Conversely, in *Hutton* those same claimed injuries were found to satisfy the injury-in-fact element because in incurring these costs, the optometrists were mitigating against a substantial risk of harm that *actually existed*, as was evidenced by the misuse of the plaintiffs’ PII that resulted in the opening of unauthorized credit cards in the optometrists’ names. Thus, *Hutton* demonstrates that mitigation costs incurred by those impacted by a data breach may be sufficient to establish the injury-in-fact prong of the standing analysis, but only where such costs were incurred in response to actual harm that had been experienced by the data breach victims in the form of actual misuse of their PII.

**THE FINAL WORD**

Ultimately, the *Hutton* decision only adds to the growing divide among the federal courts of appeal concerning the requirements for demonstrating a cognizable injury-in-fact for purposes of Article III standing in the context of data breach class action litigation. While *Hutton* does support the conclusion that a mere fear of future, uncertain injury – without more – will be inadequate to establish standing in future data breach class action suits down the road, significant uncertainty remains as to the precise showing that must be made by data breach victims in connection with a future increased threat of identity theft in order to successfully overcome the injury-in-fact standing hurdle. Unfortunately, this uncertainty may only be resolved by a definitive ruling on the issue by the U.S. Supreme Court, which would, in turn, allow for consistent application of the law across all federal courts throughout the country.