Data breaches of companies that expose consumer information are a pervasive and growing issue. The United States Courts of Appeals are divided over whether consumers have Article III Standing to sue the hacked organizations that did not protect their personal data. This Comment draws on insights from criminal law to argue that courts should take a more expansive view of the harm to consumers when their personal data is exposed, even where the plaintiffs cannot allege that their data has been misused. This approach would give more consumers the opportunity to have a day in court to vindicate the real but hard-to-define harms of exposure.

INTRODUCTION ................................................................. 258
I. CIRCUITS ARE DIVIDED OVER STANDING IN DATA BREACH CASES ................................................................. 260
   A. The Circuits That Take a More Expansive Approach to Data Breach Harms ......................................................... 264
   B. The Circuits That Take a Narrower Approach to Data Breach Harms ................................................................. 266
   C. The Third and Fourth Circuits ............................................. 268

† Comments Editor, University of Pennsylvania Law Review Volume 172; J.D. Candidate, University of Pennsylvania Carey Law School, Class of 2024; A.B., Brown University, 2019. Thank you to Professor Michael Levy for his guidance. I am grateful to Lisa Goldberg, Ken Ribet, Elena Renken, Emma Dyson, Emily Cooley, and Professor Kermit Roosevelt for comments on drafts. This comment also benefited from conversations with Stephanie Ribet, Jonathan Zisk, Nabil Shaikh, and Will McDonald. Thank you to the editors of the University of Pennsylvania Law Review Volume 172 staff for insightful comments and careful editing.
D. *The Open Question* ................................................................. 270

II. **EXISTING LITERATURE ON ARTICLE III STANDING IN DATA BREACH CASES PROPOSES NEW STANDARDS FOR THE COURTS AND THEORIZES ABOUT HARM** ........................................ 271
   A. *Proposed Standards* ............................................................. 271
   B. *Ideas About Harm* .............................................................. 274

III. **COURTS SHOULD TAKE A MORE EXPANSIVE VIEW OF HARM IN DATA BREACH CASES** ........................................... 275
   A. *Congress’s Recognition of the Harms of Identity Theft Provides Guidance.* ................................................................. 276
      1. Criminal Law ................................................................. 276
      2. Civil Enforcement ........................................................ 281
   B. *Attempted Identity Theft is Analogous to a Risk of Future Injury* ........ 282
   C. *Concentrated Criminal Attacks to One Individual Can Help to Conceptualize Small Harms to the Many* ................................. 283
   D. *Limitations of the Application of Criminal Law to Understanding Article III Standing* .................................................... 284

CONCLUSION .................................................................................. 286

INTRODUCTION

On September 15, 2022, *The New York Times* ran the headline, “Uber Investigating Breach of Its Computer Systems.”¹ It was not Uber’s first data breach.² And similar incidents are all over the news. Just six weeks earlier, on July 31, 2022: “A Cyberattack Illuminates the Shaky State of Student Privacy.” The article reported that experts were “troubled” by the extent of the reported breach, which included intimate details about students dating back more than ten years.³ These high-profile, large-scale cyberattacks occur frequently. For example, T-Mobile’s 2021 breach exposed 40 million people,⁴ Capital One’s 2019 breach exposed 98 million,⁵ and Equifax’s 2017 breach

---

² Id.
exposed 147 million users. The Federal Trade Commission ("FTC") can bring suit against those companies and hackers and even executives may face criminal charges. However, the United States Courts of Appeals are divided over what sort of injury suffices to give plaintiffs standing to sue companies for data breaches that expose their personal information and thus increase their risk of identity theft or other harms from exposure. This issue is important to consumers because when the hackers behind the breaches are unidentified, companies become the targets of litigation. There is at least some public consensus that when customer data is stolen, “it’s the company’s fault” for failing to adequately protect its systems.

Standing doctrine is a threshold issue that requires plaintiffs to show that they have been injured to get into court. The U.S. Courts of Appeals are divided about whether data breaches give rise to the kind of cognizable harm that should allow consumers to seek redress from the hacked companies. This comment argues the standard for standing in data breach cases should be relatively low because criminal law, especially federal criminal law, recognizes identity theft and hacking as serious harms.

Part I of this comment provides a brief overview of the case law and details the circuit split. Part II outlines some of the existing arguments on this topic; the discussion proposes legislative and judicial solutions, and academic theories about what the harms to consumers are. Finally, Part III explores what criminal law can teach us about the harms of a data breach, 6 Equifax Data Breach Settlement, FED. TRADE COMM’N, https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement [https://perma.cc/PUA8-HTKC] (last visited Sept. 20, 2023).

7 See, e.g., id.


9 See Beck v. McDonald, 848 F.3d 262, 273 (4th Cir. 2017) (“Our sister circuits are divided on whether a plaintiff may establish an Article III injury-in-fact based on an increased risk of future identity theft.”).

10 See Grayson Wells, Comment, What’s the Harm? Federalism, the Separation of Powers, and Standing in Data Breach Litigation, 96 IND. L.J. 937, 938 (2021) (explaining how companies become the defendants of data breach litigation when hackers are unidentified).

11 Brian X. Chen, A Breach at LastPass Has Password Lessons for Us All, N.Y. TIMES (Jan. 5, 2023), https://www.nytimes.com/2023/01/05/technology/personaltech/lastpass-breach-password-safety.html [https://perma.cc/5WXF-LR4G]; see, e.g., id. (detailing the breach of a password manager—an organization that keeps a list of a customer’s login materials on an online cloud and discloses the risks to users—and reminding readers that the company is ultimately responsible as the data custodians of sensitive information).


13 Beck, 848 F.3d at 273.
which in turn informs whether exposed consumers have experienced sufficient injuries to bring the breached companies to court. Criminal law recognizes identity theft and computer fraud as harms, penalizes attempted identity theft, and has a more expansive view of harm than civil law currently recognizes in the Article III standing context. Because standing hinges on whether consumers have been injured by the exposure of their sensitive data, the harm inquiry should be informed by related harms in the criminal space. Courts should adopt a more expansive view of injuries from data breach incidents and give consumers a wider avenue into court to seek redress for harms stemming from their exposed data.

I. CIRCUITS ARE DIVIDED OVER STANDING IN DATA BREACH CASES

First, a brief overview of the doctrinal background before addressing the application to data breach cases in the circuit courts. Article III of the Constitution gives federal courts jurisdiction over "cases" and "controversies." The doctrine of standing, a threshold issue, identifies those cases "which are appropriately resolved through the judicial process," and was developed to ensure judicial restraint. To establish a case of Article III standing, the plaintiff bears the burden of showing he has "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." The injury in fact requirement "helps to ensure that the plaintiff has a 'personal stake in the outcome of the controversy.'" To suffice, the injury must be "an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." An injury is particularized if it impacts the plaintiff in a "personal and individual way" and concrete if it "actually exist[s]," although it need not be "tangible."

14 U.S. CONST. art. III., § 2.
15 Whitmore, 495 U.S. at 155.
16 See Spokeo, Inc. v. Robins, 578 U.S. 370, 378 (2016) ("The doctrine developed in our case law to ensure that federal courts do not exceed their authority as it has been traditionally understood.").
17 Id. This comment addresses only the first prong, which is the sufficiency of the injury in data breach cases. Prongs two and three are beyond the scope of this discussion.
20 Id.
21 Id. at 340.
A risk of future injury is actual or imminent if the harm is “certainly impending.” In *Clapper v. Amnesty International*, the plaintiffs were a group of international human rights organizations who alleged a statute allowing “governmental electronic surveillance of communications for foreign intelligence purposes” had chilled their virtual communications with colleagues abroad. They claimed the statute had spurred them to take “costly and burdensome measures to protect the confidentiality of [their] sensitive communications.” The Court explained that although there was “an objectively reasonable likelihood” that their communications would be surveilled, the plaintiffs’ “theory of future injury [was] too speculative to satisfy the well-established requirement that threatened injury must be ‘certainly impending.’” While the Court held that there was no injury in fact, its language left open the possibility that a sufficiently attenuated chain of inferences could satisfy the imminence requirement in a future case.

Intangible harms can satisfy the injury requirement for Article III purposes. In *Spokeo v. Robins*, the defendant was a search engine that specialized in returning personal information about individual people by searching various online databases. The defendant’s users included employers seeking information about perspective employees. The plaintiffs were a group of individuals about whom the defendant returned inaccurate search results. For the named plaintiff, the defendant’s search incorrectly indicated that the plaintiff was married, had children, was in his fifties, was employed, held a graduate degree, and was relatively wealthy. The question for the Court was whether the plaintiff had suffered a cognizable injury. The Court explained the harm must be “concrete” and not “abstract,” declaring that an “intangible harm” can satisfy the concreteness requirement, especially if it “has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts.”

---

23 Id. at 402.
24 Id. at 401–02.
25 Id. at 406–07.
26 Id. at 401.
27 See generally id.
29 Id. at 336
30 Id. at 333.
31 Id. at 336.
32 Id. at 339.
33 Id. at 340–41.
violation” that may result in no harm, and thus remanded the case for a new analysis of the facts in light of the opinion.34

The Court further clarified the injury in fact requirement in TransUnion LLC v. Ramirez.35 The plaintiffs were consumers suing a credit reporting agency for “providing misleading credit reports” to third parties.36 At stake was more than the relatively innocuous but wrong personal details in Spokeo. Instead, the named plaintiff “learned the hard way” that he had made it onto the defendant’s list of individuals who constituted a national security threat.37 When he attempted to buy a car, the dealership refused to sell to him on the grounds that the credit check turned up his name on the “terrorist list.”38 The plaintiff sued, alleging violations of the Fair Credit Reporting Act.39 Again, the question for the court was whether the plaintiff had suffered an injury in fact.40 In holding that it had “no trouble” finding that those class members whose information had been passed onto third parties had suffered a concrete harm,41 the Court explained that the injury in fact requirement does not demand “an exact duplicate” of a traditionally recognized harm, but cautioned that Spokeo was not “an open-ended invitation” to loosen standing requirements based on evolving views about what cases federal courts should hear.42 These class members had been labeled “potential terrorists, drug traffickers, or serious criminals,” constituting a harm with a close relationship to defamation,43 “a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts”.44 But the Court declined to find standing for those consumers about whom incorrect information had not been disseminated to any third parties, analogizing the harm to that posed by a defamatory letter kept in a desk drawer and never sent to anyone.45

The TransUnion Court explicitly enumerated that where consumers allege they have been harmed by the exposure of sensitive data, the “disclosure of private information” is a harm that is both concrete and intangible.46 The Court explained that actual knowledge of a risk of harm could give rise to additional psychological and emotional harms, but declined to comment on

34 Id. at 342-43.
35 141 S. Ct. 2190, 2204 (2021).
36 Id. at 2200.
37 Id. at 2201.
38 Id. The plaintiff’s wife ultimately purchased the car in her own name. Id.
39 Id. at 2202.
40 Id. at 2204.
41 Id. at 2209.
42 Id. at 2204.
43 Id. at 2209.
45 TransUnion, 141 S. Ct. at 2210.
46 Id. at 2204.
whether these harms themselves can suffice for Article III purposes.\textsuperscript{47} These dicta are relevant because data breach litigants frequently allege emotional harms like stress or anxiety, which may seem more ethereal and are certainly harder to measure than monetary harms. Thus, this acknowledgment of mental harm—even without additional comments on whether the harm is alone enough to open the door to the courthouse—may allow plaintiffs to bring new theories of litigation to federal courts and shape Article III case law down the road.\textsuperscript{48}

Courts agree that plaintiffs who have suffered identity theft or fraud because of a data breach have standing to bring a suit against the companies that put their data at risk.\textsuperscript{49} Together, \textit{Clapper}, \textit{Spokeo}, and \textit{TransUnion} give contours to standing doctrine as applied to data breach cases where there is no showing of identity theft. \textit{TransUnion} explained that a risk of future harm can give rise to standing for the pursuit of injunctive relief as long as the risk is imminent and substantial.\textsuperscript{50} Where risk of future injury leads to a separate, concrete harm, the risk of future injury can satisfy the standing requirement.\textsuperscript{51} But when the injury is less easily defined,\textsuperscript{52} or not obviously traceable to the breach event, the circuit courts are divided over whether a data breach is a cognizable injury in fact to consumers.\textsuperscript{53} What follows is a brief overview of

\begin{itemize}
  \item \textsuperscript{47} Id. at 2211 n.7.
  \item \textsuperscript{48} See, e.g., I.C. v. Zynga, Inc., 600 F. Supp. 3d 1034, 1052-55 (N.D. Cal. 2020) (noting that the plaintiffs cited emotional distress as an injury following a data breach, but declining to find standing because these injuries can qualify as concrete only when the underlying harms are imminent or substantial).
  \item \textsuperscript{49} In their leading case on standing and data breach, \textit{Attias v. Carefirst}, the D.C. Circuit noted that “[n]obody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury.” 865 F.3d 620, 627 (D.C. Cir. 2017); see also Lauren M. Lozada, Note, The (Possibly) Injured Consumer: Standing in Data Breach Litigation, 93 ST. JOHN’S L. REV. 461, 462 (2019) (noting that, for consumers who have actually suffered some kind of fraud or identity theft from a data breach, a lawsuit is “relatively straightforward”).
  \item \textsuperscript{50} See \textit{TransUnion}, 141 S. Ct. at 2210-11 (explaining that future harm may satisfy the injury in fact element of Article III standing when one is seeking injunctive relief).
  \item \textsuperscript{51} Id.
  \item \textsuperscript{52} See, e.g., Storm v. Paytime, Inc., 90 F. Supp. 3d 159, 367-69 (M.D. Pa. 2015) (explaining that the time and transit costs a plaintiff incurred as a result of a four-hour increased commute time were not certainly impending and thus did not “create a foothold” for standing); Quintero v. Metro Santurce, Inc., No. 20-CV-01075, 2021 WL 5855752, at *4 (D.P.R. Dec. 9, 2021) (holding that plaintiffs who had sensitive data, including social security numbers, stolen in a data breach did not have standing on the ground that the alleged motive was a “garden-variety ransomware attack” rather than identity theft and there was no evidence of data misuse).
  \item \textsuperscript{53} See In re 21st Century Oncology Customer Data Sec. Breach Litig., 380 F. Supp. 3d 1243, 1250–51 (M.D. Fla. 2019) (explaining the circuit split); see also Megan Dowty, Comment, Life is Short. Go to Court: Establishing Article III Standing in Data Breach Cases, 90 S. CAL. L. REV. 683, 686 (2017) (explaining that the circuit split centers on the “risk of identity theft or fraud” and, increasingly, “‘sorting-things-out’ costs and monitoring expenditures”).
\end{itemize}
how the different circuits have dealt with the issue of standing in data breach cases.\textsuperscript{54}

\textbf{A. The Circuits that Take a More Expansive Approach to Data Breach Harms}

The First, Sixth, Seventh, Ninth, and D.C. Circuits have taken an expansive view of the harms of data breaches and held that an increased risk of identity theft and credit card fraud satisfies the injury in fact requirement. In other words, they do not require an allegation of actual misuse. For example, in In re Zappos.com, Inc., the plaintiffs were customers who had entrusted their names, phone numbers, credit card information, and other personal data to an online apparel vendor.\textsuperscript{55} After these data were exposed in a breach of the website, customers sued, arguing the company had not taken adequate steps to protect their sensitive information.\textsuperscript{56} Reasoning that the stolen data would give hackers enough materials to commit fraud or identity theft, the Ninth Circuit held that the breach placed the plaintiffs at an imminent risk of harm and concluded that the Article III injury requirement was satisfied.\textsuperscript{57}

Similarly, the Sixth Circuit recognized that an increased risk of identity theft was sufficient for standing in Galaria v. Nationwide Mutual Insurance Co.\textsuperscript{58} The Court noted that the sensitivity of the stolen data (social security numbers) placed plaintiffs at a “continuing, increased, risk of fraud and identity theft.”\textsuperscript{59} Indeed, the defendant had itself recognized this risk by providing its customers with mitigation measures.\textsuperscript{60} Thus, the court held that the plaintiffs had satisfied the injury in fact requirement.\textsuperscript{61}

The D.C. Circuit likewise concluded that where hackers had access to all the information needed to steal the plaintiffs’ identities, the affected individuals faced a substantial risk of fraud and had thus suffered a cognizable injury in fact.\textsuperscript{62} The hackers stole fingerprints, social security numbers, and

\textsuperscript{54} The majority of these cases was decided before TransUnion, which suggests that this area is likely to evolve significantly in the coming years. Note also that the Tenth and Fifth Circuits have not yet addressed this issue.
\textsuperscript{55} 888 F.3d 1020, 1023 (9th Cir. 2018).
\textsuperscript{56} Id.
\textsuperscript{57} Id. at 1028-29.
\textsuperscript{58} 663 F. App’x 384 (6th Cir. 2016). The Sixth Circuit has not yet addressed this issue precentdentially.
\textsuperscript{59} Id. at 388.
\textsuperscript{60} Id.
\textsuperscript{61} Id. at 388-89.
birthdays, among other personal data. The Court explained that it “hardly takes a criminal mastermind to imagine how such information could be used to commit identify theft.” The Court noted first that birthdays and fingerprints are immutable and social security numbers and addresses are relatively immutable. Next, the Court pointed out that some plaintiffs’ data had already been misused. Thus, the risk of future identify theft was substantial and gave rise to standing.

Most recently, the First Circuit held that, even in the absence of allegations of misuse, an imminent and substantial future risk of injury following a data breach can give rise to standing. In Webb v. Injured Workers Pharmacy, LLC, the plaintiffs sued Injured Workers Pharmacy, a pharmacy home-delivery service, following a data breach. Some plaintiffs saw evidence of data misuse (like the fraudulent filing of a tax return); other plaintiffs did not and alleged emotional harms and mitigation measures. The Court first held that actual misuse of data was an injury in fact both because of the temporal connection between the evidence of the misuse and the analogy of the alleged to the tort of invasion of privacy. Then, the Court held that while his case was “more difficult,” the plaintiff who had not alleged actual misuse of data had a concrete injury “based on the material risk of future misuse of [his] [personal identifying information] and a concrete harm caused by exposure to this risk.” Such a risk “may be heightened where the compromised data is particularly sensitive.” The Court explained that the time and energy the plaintiffs spent protecting themselves from future risk, time which could “otherwise have been put to some productive use,” was a concrete injury sufficient to confer standing.

63 Id. at 56.
64 Id.
65 Id.
66 Id.
67 Id. at 59.
68 Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365, 376 (1st Cir. 2023). Webb revisited the Court’s prior leading case, Katz v. Pershing, LLC, 672 F.3d 64 (1st Cir. 2012), which held that the plaintiff’s “hypothesis that at some point an unauthorized, as-yet unidentified, third party might access her data and then attempt to purloin her identity” was not sufficient to give rise to standing. Id. at 80. Indeed, the plaintiff had not even alleged actual access of here data. Id. at 79.
69 Webb, 672 F.4th at 369–70.
70 Id. at 370.
71 Id. at 372–74. Recall that the Spokeo Court emphasized that harms with a close relationship to a traditionally recognized basis for a lawsuit were more likely to give rise to standing. Spokeo v. Robins, 578 U.S. 330, 341 (2016).
72 Webb, 72 F.4th at 374.
73 Id. at 376.
74 Id. at 376–77.
The Seventh Circuit—arguably the most liberal circuit on this issue—has recognized both an increased risk of harm or fraud and investment in mitigation measures as injuries that satisfy Article III standing. In *Lewert v. P.F. Chang's China Bistro, Inc.*, the plaintiffs had credit card numbers stolen in a restaurant chain's data breach.\(^75\) The court held that although one of the plaintiffs had not yet been a victim of fraud because there were no charges on his account, the “time and effort” spent resolving the issue and the mitigation costs were sufficient to satisfy standing.\(^76\) The court explained that the increased risk of fraud and identity theft were also cognizable injuries that would support standing because of the incentive for hackers to make use of the data as soon as possible.\(^77\)

B. The Circuits That Take a Narrower Approach to Data Breach Harms

By contrast, the Second, Eighth, and Eleventh Circuits disfavor standing in the absence of a direct showing of theft or fraud, despite allegations of increased risk, mitigation measures, or emotional harms.

The Eighth Circuit requires a showing of actual data misuse for a plaintiff to have standing. In its leading case, *In re SuperValu, Inc.*, the plaintiffs were customers who alleged their credit card information was stolen in two cyberattacks.\(^78\) In its analysis of whether the plaintiffs had standing, the court divided the plaintiffs into those who had alleged misuse of data and those who alleged only an increased risk of fraud, finding standing for the former group but not for the latter.\(^79\)

The Eleventh Circuit followed similar reasoning in its leading case, *Tsao v. Captiva MVP Restaurant Partners, LLC*, holding that neither mitigation measures nor a risk of data misuse were sufficient injuries for Article III standing purposes, although the breach had exposed the plaintiffs’ sensitive financial information.\(^80\) There, the defendant, a restaurant, collected

\(^75\) 819 F.3d 963, 965 (7th Cir. 2016).

\(^76\) Id. at 967. The Court cited *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 694 (2015), which “found injuries sufficient for standing in the time and money the class members predictably spent resolving fraudulent charges” and protecting against the risk of future identity theft or fraudulent charges. *Lewert*, 819 F.3d at 966-67. Here, the plaintiffs spent time and effort resolving fraudulent charges, purchasing credit-card monitoring, and reviewing credit card statements for fraudulent activities. *Id.* at 967.

\(^77\) Id.

\(^78\) 870 F.3d 763, 766 (8th Cir. 2017). The stolen information included names, account numbers, expiration dates, card verification value codes, and personal IDs. *Id.*

\(^79\) Id. at 768-74. That financial information, without accompanying identifying data, is less likely than names and social security numbers to be used for theft, may have been dispositive in this case. *Id.* at 770-71.

\(^80\) 986 F.3d 1332, 1343-45 (11th Cir. 2021) (“We are persuaded by the reasoning of the Eighth Circuit in SuperValu, and the facts of that case map closely to the facts of this one.”).
customer credit and debit card information. These data were exposed following a data breach. The Court explained that the mere increased risk of identity theft, the failure to allege actual data misuse and the plaintiff’s immediate cancelation of his credit card were fatal to standing. Likewise, the plaintiff’s time and energy spent canceling these cards were not an injury and amounted to “inflicting injuries on himself to avoid an insubstantial, non-imminent risk of identity theft.”

The Second Circuit’s recent opinion, McMorris v. Carlos Lopez & Associates, LLC, might give us an indication of where the law is going. The defendant was an employer that accidentally emailed a spreadsheet containing sensitive information to sixty-five employees. The information included social security numbers, home addresses, cell phone numbers, educational degrees, and dates of hire of more than 100 employees. Based on a thorough synthesis of the case law developed in its sister Circuits, the court developed a three-factor test for whether plaintiffs at an increased risk of theft or fraud have alleged an injury in fact. The court considered (1) whether the exposure resulted from “a targeted attempt to obtain that data”; (2) whether there is evidence that the data “has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud”; and (3), whether the data “is sensitive such that there is a high risk of identity theft or fraud.” In addition, the court discussed whether investments in data breach mitigation constitute an injury in fact, concluding that steps like

---

81 Id. at 1335.
82 Id.
83 Id. at 1333-34.
84 Id. at 1345.
85 For example, the case has been cited in many leading Circuit cases cited the case. See, e.g., Clemens v. ExecuPharm Inc., 48 F.4th 146, 153–54 (3d Cir. 2022) (analyzing standing of plaintiff in connection with data breach through the lens of the three-factor test laid out in McMorris); Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365, 375–77 (1st Cir. 2022) (considering the McMorris factors in standing inquiry wherein plaintiff alleged that pharmacy had suffered a data breach). The Eleventh Circuit also cited it in In re Equifax Customer Data Sec. Breach Litig., 999 F.3d 1247, 1263 (11th Cir. 2021) for the proposition that a risk of future injury is more likely to suffice for Article III purposes where the plaintiff can show evidence of misuse. See also Andrew Ridge, Note, Standing in the Ether: Constitutional Standing in Data Breach Cases After McMorris, 17 BROOK. J. CORP. FIN. & COM. L. 219, 221 (2022) (“[T]he Second Circuit attempted to put the controversy to rest.”).
87 Id.
88 Id. at 303.
89 Id.
paying for a credit monitoring service\textsuperscript{90} are a way to manufacture standing rather than a true injury.\textsuperscript{91}

Under the specific facts in \textit{McMorris}, the court concluded that the plaintiffs did not have standing because they had not alleged actual access by a malicious third party, misuse, or a sufficiently substantial risk of theft or fraud.\textsuperscript{92} Although the court did not say so explicitly, it was likely important that the email was sent only to internal employees rather than stolen by or exposed to malicious outsiders, given the data was the kind that puts victims “at a substantial risk of identity theft or fraud.”\textsuperscript{93} On balance, the Second, Eighth, and Eleventh Circuits have taken a narrower view of the harms to consumers in data breach events, and have demanded a higher showing of harm in the Article III context than the more liberal Circuits discussed above.

\textbf{C. The Third and Fourth Circuits}

The Third and Fourth Circuits have carved out something of a middle ground. In \textit{Clemens v. ExecuPharm Inc.}, the plaintiff’s former employer suffered a data breach that exposed its employees’ sensitive information, such as their social security numbers, addresses, and financial information.\textsuperscript{94} Evaluating some of the principles distilled by the \textit{McMorris} court, the court held that the \textit{Clemens} plaintiffs alleged a sufficiently imminent harm.\textsuperscript{95} Furthermore, in light of the guidance in \textit{TransUnion},\textsuperscript{96} the court held that an increased risk of future theft or fraud is sufficient for Article III concreteness so long as the plaintiff has “allege[d] that the exposure to that substantial risk that the exposure to that substantial risk

\begin{itemize}
  \item \textsuperscript{90} A credit monitoring service provides alerts to the user where there are changes to the user’s credit profile and monitors the dark web for evidence of fraud. For example, if someone opens a new credit account, for example, the user will be made aware.
  \item \textsuperscript{91} \textit{Id.}
  \item \textsuperscript{92} \textit{Id. at} 303-05.
  \item \textsuperscript{93} \textit{Id. at} 303-04.
  \item \textsuperscript{94} \textit{Clemens v. ExecuPharm Inc.}, 48 F.4th 146, 150 (3d Cir. 2022). Note that this case revisited the court’s prior holding in \textit{Reilly v. Ceridian Corp.}, 664 F.3d 38 (3d Cir. 2011). \textit{Clemens}, 48 F.4th at 153. In \textit{Reilly}, the court took a somewhat more conservative view, declining to find standing either based on “allegations of hypothetical, future injury,” 664 F.3d at 42, nor based on “alleged time and money expenditures.” \textit{Id. at} 46. Although the \textit{Clemens} court distinguished its facts from those considered by the \textit{Reilly} court because, there, the risk was too speculative, the \textit{Clemens} court arguably took a broader view of what injury satisfies the imminence requirement for standing. \textit{Clemens}, 48 F.4th at 153-54 (articulating “a number of factors” to consider in determining whether an injury is sufficiently imminent to confer standing in the context of data breaches). Because of the decade-long gap between the two cases, the Third Circuit had the opportunity to revisit its precedent in light of both new Supreme Court cases and evolving case law in sister circuits. See \textit{id.} (citing \textit{Spokeo} and \textit{McMorris}).
  \item \textsuperscript{95} \textit{Clemens}, 48 F.4th at 157. For a discussion of \textit{McMorris}, see notes 85–93 and accompanying text.
  \item \textsuperscript{96} See \textit{TransUnion LLC v. Ramirez}, 141 S. Ct. 2190, 2211 (2021) (clarifying that a "mere risk of future harm" alone may not be enough to establish Article III standing when the suit is for damages).
\end{itemize}
caused additional, currently felt concrete harms” such as “emotional distress” or costly “mitigation measures.”

Likewise, the Fourth Circuit held in *Hutton v. National Board of Examiners in Optometry, Inc.* that plaintiffs had standing to sue, partially on the basis of mitigation or preventative costs where there is a substantial risk of future harm.\(^97\) The facts were those of a paradigmatic data breach case: the plaintiffs alleged that their data had been stolen in the data breach of the defendant’s database of personal information.\(^98\) One of the plaintiffs was advised by a credit card monitoring service she purchased in response to the data breach that her credit card score had fallen noticeably as a result of a fraudulent credit card application.\(^99\) Another plaintiff received a credit card for which she had not applied and which was opened under her maiden name.\(^100\) The court reasoned that the plaintiffs had already been “concretely injured” because fraudsters had both “used” and “attempted to use” the sensitive information.\(^101\)

The Fourth Circuit’s influential case, *Beck v. McDonald*, gives us an idea of what a “substantial risk” is.\(^102\) There, the court concluded that, even if it accepted the allegation that one-third of the plaintiffs would become victims of identity theft, the fact that two-thirds would suffer no harm undermined a claim of a substantial risk of harm for the group.\(^103\) But the Fourth Circuit distinguished *Hutton* from *Beck* because in *Hutton*, the plaintiffs alleged more than a mere risk, as fraudsters had already attempted to use the stolen data.\(^104\) Because the injuries were not speculative, the mitigating measures were enough to constitute injury in fact for standing.\(^105\)

---

\(^97\) Clemens, 48 F.4th at 155-56.

\(^98\) *Hutton v. Nat’l Bd. of Exam’rs in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018). It caveated this holding by saying these costs would not satisfy the injury in fact requirement when the injury is speculative. *Id.*

\(^99\) *Id.* at 616.

\(^100\) *Id.* at 618.

\(^101\) *Id.* at 617.

\(^102\) *Id.* at 622.

\(^103\) See *Beck v. McDonald*, 848 F.3d 262, 275-76 (4th Cir. 2017) (finding that, even if one third of people impacted by data breaches become victims of identity theft, “statistic [fell] far short of establishing a ‘substantial risk’”).

\(^104\) *Id.*

\(^105\) See *Hutton v. Nat’l Bd. of Exam’rs in Optometry, Inc.*, 892 F.3d 613, 621-22 (noting that these attempted uses amounted to “already suffered actual harm in the form of identity theft and credit card fraud”).

\(^106\) *Id.* at 622.
D. The Open Question

Everyone agrees that where a victim has her identity stolen as a direct and obvious consequence of a data breach, she has standing to sue the company responsible for her data.\footnote{See Attias v. Carefirst, Inc., 865 F.3d 620, 624 (7th Cir. 2017) ("Nobody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury.").} The open question is whether victims have standing where the harms are more subtle (like risk or anxiety), or not as easily traced to the breach. As courts and scholars have noted, the so-called circuit split might not be driven by a “fundamental disagreement on the law”\footnote{In re 21st Century Oncology Customer Data Sec. Breach Litig., 380 F. Supp. 3d 1243, 1251 (M.D. Fla. 2019); see also Andrew Grindstaff, Comment, Article III Standing, the Sword, and the Shield: Resolving a Circuit Split in Favor of Data Breach Plaintiffs, 29 WM. & MARY BILL RTS. J. 851, 865 (2021) ("Upon closer examination, the circuit split is much more nuanced and potentially not a true split after all.").} and instead by factual context.\footnote{See, e.g., In re 21st Century Oncology Customer Data Sec. Breach Litig., 380 F. Supp. 3d at 1254-55 (identifying three non-exhaustive factors courts can use to distill whether the plaintiff has suffered an injury in fact: ")(1) the motive of the unauthorized third-party who accessed or may access the plaintiff’s sensitive information, (2) the type of sensitive information seized, and (3) whether the information was actually accessed and whether there have been prior instances of misuse stemming from the same intrusion"); Beck, 848 F.3d at 277-78 ("The most that can be reasonably inferred . . . is that the Plaintiffs could be victimized by a future data breach. That alone is not enough.").} However, there are no bright line rules as to whether Article III standing requires an allegation of data misuse or whether psychological harms or mitigation costs satisfy the injury in fact requirement. For example, there are cases where there is evidence of misuse of data and courts nevertheless declined to find an injury,\footnote{See, e.g., Bradix v. Advance Stores Co., Inc., 2016 WL 3617717 at *1, *4 (E.D. La. July 6, 2016) (declining to find standing although the plaintiff alleged unauthorized attempts to secure financing on his credit report following a data breach).} and other cases where the plaintiffs alleged harms besides identity theft and were held to have standing to bring the case.\footnote{See, e.g., Clemens v. ExecuPharm Inc., 48 F.4th 146, 155-56 (finding that a plaintiff’s increased risk of identity theft coupled with an investment of time and money to mitigate potential harm gave rise to standing under TransUnion v. Ramirez).}

As many scholars and courts have already concluded, the most important factors are the type of data stolen and which parties get access to them.\footnote{See Part II.} Social security numbers, dates of birth, and financial information lead to a much higher risk of harm than an indication of whether the individual is affluent or married. In addition, a lost device containing social security numbers or financial information creates no risk to anyone if it is sitting in a desk drawer.\footnote{This was the court’s reasoning in Beck. See 848 F.3d 262, 274 (4th Cir. 2017) (discussing how the lack of evidence that information contained on “likely” stolen laptop was used for any malicious purpose is a reason for not finding standing).}

As many scholars and courts have already concluded, the most important factors are the type of data stolen and which parties get access to them.\footnote{See Part II.} Social security numbers, dates of birth, and financial information lead to a much higher risk of harm than an indication of whether the individual is affluent or married. In addition, a lost device containing social security numbers or financial information creates no risk to anyone if it is sitting in a desk drawer.\footnote{This was the court’s reasoning in Beck. See 848 F.3d 262, 274 (4th Cir. 2017) (discussing how the lack of evidence that information contained on “likely” stolen laptop was used for any malicious purpose is a reason for not finding standing).}
a malicious crime, a plaintiff should still have standing if his sensitive information turns up on the web and he is at a seriously elevated risk of identity theft. Lastly, because sensitive information like a social security number retains its value to a hacker over time, purchasing a credit monitoring service should give rise to standing because it will allow the victim to (1) know if he has been harmed and (2) respond promptly.

This analysis can be strengthened by an inquiry into related harms recognized by criminal law. As I explain in Part III, this methodology is instructive because Congress’s elevation of harms, while not dispositive, can inform the approach courts take to questions of Article III standing. On balance, criminal law’s recognition of harm weighs toward a more liberal standard for standing in the data breach context.

II. EXISTING LITERATURE ON ARTICLE III STANDING IN DATA BREACH CASES PROPOSES NEW STANDARDS FOR THE COURTS AND THEORIZES ABOUT HARM

Several academic papers and student comments have taken up the issue of standing in data breach cases. Much of the literature has proposed new standards for courts to apply or urged Congress to enact a federal cause of action and regulate data privacy more closely. In addition, some scholars compare the harms caused by data breaches to harms recognized by other claims.

A. Proposed Standards

Authors and courts mostly agree that the “circuit split” is driven more by factual context than by a real legal disagreement, although some circuits have been more amenable to an expansive view of harm than others.114 Thus, many of the proposals generally do not choose a side in the split per se, but instead distill guiding principles down to tests or bright line rules that the Court could adopt to provide lower courts and litigants with consistency and guidance. To name one such discussion, Devin Urness draws on principles distilled by the courts and argues for a three factor test for courts to determine whether there is a sufficiently substantial risk to a litigant: (1) the purpose created a standing issue). And indeed, this was the analogy raised by the TransUnion Court. TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2210 (2021) (“The mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party, causes no concrete harm . . . . [T]he plaintiffs’ harm is roughly the same, legally speaking, as if someone wrote a defamatory letter and then stored it in her desk drawer. A letter that is not sent does not harm anyone, no matter how insulting the letter is.”).

114 See Part I; see also Grindstaff, supra note 108, at 861-64 (categorizing circuits in those with “expansive” or “narrow” theories of data breach harms).
intentionality of the breach, (2) the type of data exposed, and (3) whether part of the data set has been misused.\(^{115}\) Notably, this three-factor test mirrors the one later adopted by the Second Circuit in *McMorris*, discussed in part I.B.\(^{116}\) Because many litigants would be “left behind” by his proposed test, Urness also suggests creating a federal right of action for consumers.\(^{117}\) If this proposal were taken up by the legislature, he argues, it would remedy judicial inaction.\(^{118}\) One possible downside of this otherwise appealing proposal is that a right of action could open the floodgates for litigation.

A narrower approach to standing is offered by another student comment, which proposes standing only where there is a showing of actual identity theft and where the plaintiff has incurred reasonable costs on mitigation measures.\(^{119}\) The author, Megan Dowty, suggests that this standard would result in payments that hold the breached organizations accountable for the losses and reimburse plaintiffs for theft or fraud only once they actually sustain a loss\(^{120}\) or incur costs on reasonable monitoring services.\(^{121}\) She notes, however, the practical limitations of recognizing mitigation measures as a cognizable injury, arguing that these types of harms are hard to quantify and define and are not sufficiently justified.\(^{122}\)

Some papers have tried to simplify the approach by offering a true bright line. Andrew Grindstaff’s student comment took an expansive view of the harm of exposure, arguing that a data breach alone is enough to establish injury in fact, recognizing that “once [the] data has been stolen, the threat to victims is permanent.”\(^{123}\) This argument takes a long-term view of the harm


\(^{116}\) 995 F.3d 295, 303 (2d Cir. 2021). The intentionality of the breach matches the Second Circuit’s first factor (whether the breach resulted from a “targeted attempt to obtain that data”). *Id.*

\(^{117}\) Id. at 1520.

\(^{118}\) Id. at 1521.

\(^{119}\) See Dowty, *supra* note 53, at 701-02 (arguing that only unremedied costs should be compensable).

\(^{120}\) *Id.* at 703 (“Recognizing injury only where plaintiffs have incurred actual, unremedied costs would result in more accurate and fair damages and reduce overlap in damages between financial institutions and individual plaintiffs.”).

\(^{121}\) *Id.* at 704 (“Money spent on monitoring services results in a concrete, particularized, and redressable injury, and it should be compensated as such, so long as the costs are reasonable. Therefore, failure of a hacked company to reasonably provide customers with monitoring services should constitute a cognizable injury.”).

\(^{122}\) *Id.* at 712.

of increased risk. Likewise, Parker Hudson’s comment urges the Supreme Court to offer a bright-line rule to consumers, suggesting that the risk of future identity theft “is either sufficient to establish Article III standing or it is not.” Hudson argues that a broader view of harm better conforms to precedent. Like other scholarship, however, the comment notes that “meaningful clarification will more likely come from Congress,” and goes on to propose a federal cause of action. While superficially appealing, these simplistic approaches do not grapple with the fact that not all data are created equally. The theft of a social security number is more alarming and harmful than standard socioeconomic data, such as gender, marital status and income level. While that consumer may not want his information out in the world, it is less likely to lead to monetary harm or identity theft than other, more sensitive information, like his address and bank account information.

Some research has taken a company-centric approach to the discussion. To name one example, Lauren Lozada’s student comment urges courts to balance giving consumers an avenue of recovery after a data breach incident with fairness to the companies that have been hacked. Lozada notes that companies are themselves victims of hackers and may have been breached although they made “every good faith effort” to protect their customers’ data. Her solution would take into account the likelihood of injury and the efforts of the company to protect the data. If adopted, this standard would recognize standing only when injury is likely and the company has done little to protect itself from hackers. Grindstaff’s comment notes that even if everyone agrees that the consumers could sue the party responsible for the data, it is not clear which party that is. All of these discussions reflect the idea that exposed customers have experienced a real harm, but the solutions reflect considerations beyond vindicating injury. They factor in consistency, the ability of the company to

125 Id. at 559.
126 Id.
127 Id. at 478-79 ("On one hand, consumers should have some avenue of redress when their data is stolen through no fault of their own. On the other, companies that fall victim to a breach are just that—victims").
128 Id. at 479.
129 Id. at 484-85.
130 Id.
131 Grindstaff, supra note 108, at 871-72 (explaining that hackers can target the entity running the cloud instead of the entity that owns the data).
132 Id.
protect consumers, whether consumers are likely to be compensated without litigation, and which party is best positioned to bear the risk.

B. Ideas About Harm

Scholars have recognized that a future risk of injury and emotional harm can constitute injuries and have suggested that there are methods of measuring these harms. In their paper, *Risk and Anxiety: A Theory of Data-Breach Harms*, Professors Daniel Solove and Danielle Citron study the harms caused by data breaches.\(^{133}\) Identifying harm as the “defining issue” of data breach litigation,\(^{134}\) they dive into theoretical ideas about both risk and anxiety as harms.\(^{135}\) The authors offer a “sufficiently concrete” approach to measuring these apparently abstract injuries.\(^{136}\) Echoing the approach of other scholars and many courts, Solove and Citron conclude that risk can be evaluated by factoring in the likelihood and magnitude of future injury, the sensitivity of the data, whether other actions are likely to mitigate the potential harm, and the reasonableness of any mitigative investments of consumers.\(^{137}\) Finally, after arguing that “emotional distress should count as a sufficient basis to establish harm,” they conclude that courts should engage in a fact-heavy inquiry to decide whether the emotional distress is reasonable under the circumstances.\(^{138}\)

Professor David Opderbeck, by contrast, argues that “a general category of dignitary or emotional harm is a poor doctrinal fit for most kinds of data breaches.”\(^{139}\) He explains that while anxiety about exposed private information is appropriate, that emotional response is not easily tied to one breach.\(^{140}\) Rather, it is a consequence of systemic issues with cybersecurity and cybercrime.\(^{141}\) He acknowledges that “[t]rue identity theft” can produce “tangible emotional stress” because it can be a challenge to untangle.\(^{142}\) But


\(^{134}\) Id. at 739.

\(^{135}\) See id. at 756. Solove and Citron discuss different areas of the law that have evolved to recognize a risk of future harm from environmental regulation to medical malpractice. Id. at 761-64. They also note that many areas of the law accommodate “‘ethereal’ harms,” from assault and privacy torts to fear of contracting diseases. Id. at 767-74.

\(^{136}\) Id. at 773-74.

\(^{137}\) Id. at 774-77.

\(^{138}\) Id. at 776-77.


\(^{140}\) Id. at 1038 (analogizing a data breach to a toxic tort for which “there is no way to tie that anxiety to one catastrophic plastic spill”).

\(^{141}\) Id. (acknowledging that both a toxic tort and a data breach produce “systemic, not individualized, harm[s]”).

\(^{142}\) Id. at 1039.
while “low-level identity theft” like the theft and use of credit card information might be “annoying and unpleasant,” it is nonetheless unavoidable in our modern economy and mostly happens without any human being viewing the private information.143

He argues that other consequences of data breach, like synthetic identity theft (the use of someone’s private information to construct a fake person), market manipulation, trade secret theft, and state surveillance are also unlikely to produce emotional harms.144 He writes that “[t]he average reasonable American consumer in cyberspace, therefore, should not become seriously distressed by a data breach notification.”145 A breach should give rise to “some prudent awareness rather than panic.”146

The existing literature about standing in the data breach context is informative because it offers insight into what the harm really is to consumers while also wrestling with practical approaches to recognizing these injuries in court.

III. COURTS SHOULD TAKE A MORE EXPANSIVE VIEW OF HARM IN DATA BREACH CASES

In Part III, I add to the discussion by taking a close look at harm in an adjacent arena: criminal law. Congress’s judgment in general and in criminal law in particular illustrates the materiality of the harm felt by exposed plaintiffs in data breach cases. I argue that risk of identity theft is a cognizable harm based on what the legislatures have chosen to criminalize.147

In federal court, hackers are generally charged with violating 18 U.S.C. § 1030, the Computer Fraud and Abuse statute (“CFAA”).148 The CFAA criminalizes, among other conduct, intentional access of a computer without authorization and obtaining information from any protected computer, among other conduct.149 Furthermore, every state has a criminal law covering

---

143 Id.
144 Id. at 1040.
145 Id. at 1066.
146 Id.
identity theft, and there is a federal criminal identity theft statute, 18 U.S.C. § 1028. These statutes shed light on our legislators’ views of cyber harms. While the Court cautioned in Spokeo that Congress’s “identifying and elevating intangible harms” does not mean a plaintiff has standing whenever the legislature has recognized a harm either through a criminal statute or a civil cause of action, the Court also acknowledged that “Congress is well positioned to identify intangible harms,” and its judgment is “instructive and important.” Indeed, “criminal law attributes major significance to the harm actually caused by a defendant’s conduct.” Even if the analogy is imperfect, it is instructive because it brings a degree of concreteness to an abstract inquiry.

A. Congress’s Recognition of the Harms of Identity Theft Provides Guidance

Congress has recognized the harms of data breaches both in the criminal context, which is the focus of this paper, and elsewhere in the civil context. I write mostly about criminal law, and I also offer a brief discussion of the FTC’s enforcement power.

1. Criminal Law

First, the existence of the CFAA and § 1028 illustrates that Congress has recognized identity theft and data breaches as serious harms worthy of vindication. Section 1028 criminalizes, among other acts, knowing transfer, possession, or use of someone else’s means of identification with intent to commit or in connection with any other violation of the law. The seriousness with which Congress takes identity theft is shown by the fact that the maximum prison sentence for transfer, possession, or use of a means of identification is fifteen years if the actor obtains “anything of value aggregating $1,000 or more” in a year-long period. Aggravated identity theft, 18 U.S.C. § 1028A, which is identity theft that takes place during and

---

152 578 U.S. at 341; accord TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2204-05 (2021) (explaining that while courts must “afford due respect” to Congress’s elevation of harms, they nonetheless must decide independently whether a harm is sufficiently concrete in the Article III context).
155 Id. § 1028(b)(1).
in relationship to one of a number of enumerated federal offenses, carries a
mandatory minimum sentence of two years.\textsuperscript{156}

Many sections of the CFAA apply to hacking conduct, including § 1030(a)(2)(C), which criminalizes intentional access of a computer without
authorization and obtaining information.\textsuperscript{157} Depending on the conduct in
question, defendants can face up to ten years in prison if they are found guilty
of violating § 1030.\textsuperscript{158} The statutory maximum punishment is relevant to a
discussion of harm because the Supreme Court has explained that the most
relevant criterion with which to assess the seriousness of an offense is “the
judgment of the legislature, primarily as expressed in the maximum
authorized term of imprisonment.”\textsuperscript{159} It is clear from the face of the statute
that Congress takes harms stemming from identity theft and hacking
seriously. The legislative history lends support to this reading.

The legislative history of the federal identity theft statute sheds light on
Congress’s view of the harm that personal data misuse can cause. The Senate
report on the 1998 Identity Theft and Assumption Deterrence Act, quoting
FTC testimony, explained that the harm of identity theft is “exacerbated
because consumer victims have difficulty obtaining help from law
enforcement since the law does not recognize these individuals as victims.”\textsuperscript{160}
The report noted that “anecdotal evidence suggests that Internet growth
increases opportunities for criminal activity.”\textsuperscript{161}

This legislative history explicitly acknowledged that the legal system
underrecognizes identity theft victims—an issue that lowering the civil
barriers into court would help to address, because plaintiffs could seek
compensation from the companies that put their data at risk, even if the
malicious third party is nowhere to be found. The legislative history also
explicitly acknowledged the human cost of identity theft, explaining that
these “costs include emotional costs, as well as financial and/or opportunity
costs. For example, the victims may be unable to qualify for a mortgage.”\textsuperscript{162}
Senator Patrick Leahy reflected on the “severe” consequences faced by
victims.\textsuperscript{163} These ranged from ruined credit ratings that impacted the ability
of victims to get credit cards or loans, to debts incurred in their names, to

\begin{itemize}
\item \textsuperscript{156} Id. § 1028A(a)(1).
\item \textsuperscript{157} Id. § 1030(a)(2)(C).
\item \textsuperscript{158} Id. § 1030(c)(1)(A).
\item \textsuperscript{159} Lewis v. United States, 518 U.S. 322, 327 (1996); see id. (explaining the seriousness of
offenses in the jury trial context).
\item \textsuperscript{160} S. REP. NO. 105-274, at 6 (1998).
\item \textsuperscript{161} Id.
\item \textsuperscript{162} Id. (citing U.S. GEN. ACCT. OFF., GAO/GGD-98-100BR, IDENTITY FRAUD:
INFORMATION ON PREVALENCE, COST, AND INTERNET IMPACT IS LIMITED 4 (1998)).
\item \textsuperscript{163} Id.
\end{itemize}
arrests from crimes they did not commit.\textsuperscript{164} “It can take months or even years, and agonizing effort” for victims “to clear their good names.”\textsuperscript{165}

The House committee report on the Identity Theft Penalty Enhancement Act, which amended § 1028, also identified “the growing problem of identity theft,” and explained the legislation was aimed at establishing penalties when the theft is connected to or in the furtherance of other crimes.\textsuperscript{166} Hacking targeted at stealing personal information through data theft is exactly the kind of situation explicitly contemplated in the legislative history of this amendment.\textsuperscript{167}

Data breaches—especially those that expose sensitive, personal data, like social security numbers—can be characterized as an attempted identity theft on a large scale.\textsuperscript{168} This analogy underscores the value of using criminal law to better understand the standing inquiry. As the Seventh Circuit has pointed out, “it is plausible to infer that the plaintiffs have shown a substantial risk of harm,” asking, “[w]hy else would hackers break into a store’s database and steal consumers’ private information?”\textsuperscript{169} In the leading Ninth Circuit data breach and standing case,\textit{In re Zappos.com}, the court focused on plaintiffs who had not alleged having already suffered identity theft at the time of the lawsuit.\textsuperscript{170} The court reasoned that the harm to those plaintiffs “who [had] alleged that the hackers had already commandeered their accounts or identities using information taken from Zappos . . . undermine[d] Zappos’s assertion that the data stolen in the breach cannot be used for fraud or identity theft.”\textsuperscript{171} Thus, the court held there was a substantial risk of harm to those plaintiffs whose identities had not yet been stolen.\textsuperscript{172} The case reformulates our thinking about data breach as one large identity theft event where some of the plaintiffs are victims of attempted identity theft and others are victims of “successful” fraud. Section 1028, the criminal identity theft statute, imposes the same penalties for attempt as for successful commission of any of the enumerated crimes.\textsuperscript{173} And because criminal law focuses on actual harm

\begin{itemize}
\item \textsuperscript{164} Id. at 16.
\item \textsuperscript{165} Id.
\item \textsuperscript{166} H.R. REP. NO. 108-628, at 25 (2004) ("This legislation will establish penalties for aggravated identity theft when the theft is related to or in the furtherance of certain other criminal acts.").
\item \textsuperscript{167} Id. at 11.
\item \textsuperscript{168} Amanda Draper, \textit{Identity Theft: Plugging the Massive Data Leaks with a Stricter Nationwide Breach-Notification Law}, 40 J. MARSHALL L. REV. 681, 681 (2007) ("While identity theft can occur through the theft of a person’s wallet, it can also occur through a massive security breach.").
\item \textsuperscript{169} Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (holding the plaintiffs have alleged an injury fact due to an increased risk of identity theft from a data breach.)
\item \textsuperscript{170} \textit{In re Zappos.com}, Inc., 888 F.3d 1020, 1023-24 (9th Cir. 2018).
\item \textsuperscript{171} Id. at 1027.
\item \textsuperscript{172} Id. at 1029.
\item \textsuperscript{173} See 18 U.S.C. § 1028(f).
\end{itemize}
to victims, that attempted identity theft carries the same penalties as completed identity theft suggests that Congress views the harm from both crimes as similar, if not equivalent.174

In the identity theft statute, Congress elevated four categories of “means of identification” which bolster a claim of standing for plaintiffs who have suffered exposure of data within those categories. The type of data stolen is often important, if not dispositive, in an analysis of whether the data exposure injury is concrete or the risk of future harm is imminent and certainly impending.175

Section 1028, the identity theft statute, defines four categories of means of identification:

(A) name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(C) unique electronic identification number, address, or routing code; or

(D) telecommunication identifying information or access device (as defined in section 1029(e)).176

Category (A) encompasses many of the forms of identification that are most obviously useful for identity theft (like IDs and social security numbers). Category (C) includes email addresses, and (D) includes credit and debit cards.177 While biometric data privacy and standing has been

---


175 Compare Kylie S. v. Pearson PLC, 475 F. Supp. 3d 841, 846-47 (N.D. Ill. 2020) (exposed names, emails, and dates of birth were not sensitive enough to confer standing because they were “far less likely to facilitate identity theft” than credit card information), and Dugas v. Starwood Hotels & Resorts Worldwide, Inc., No. 3:16-cv-00014, 2016 WL 6523428, at *5 (S.D. Cal. Nov. 3, 2016) (finding there was not an injury in fact because the stolen data was limited to the Plaintiff’s name, address, and credit card information for a since-canceled credit card and thus there was not a credible risk of future injury), with Portier v. NEO Tech. Sols., No. 3:17-cv-30111, 2019 WL 7946103, at *8 (D. Mass. Dec. 31, 2019) (noting that a data breach resulted in the disclosure of social security numbers which are rarely replaced, and ultimately concluding the risk of harm was serious enough to satisfy the injury requirement).


177 The statute defines a “card” as something that can be used to obtain “goods, services, or any other thing of value.” 18 U.S.C. § 1029(e)(1). Thus, a credit card is an access device. See United States v. Lyons, 556 F.3d 703, 708 (8th Cir. 2009) (explaining that a counterfeit credit card is an access card because it is a card that can be used to obtain things of value).
litigated in related contexts,\textsuperscript{178} no case has directly addressed whether exposure of biometric data is sufficient to confer standing, although one will almost certainly come to the federal courts soon. The sensitivity of the exposed data is an important part of the standing inquiry.\textsuperscript{179} Thus, that these categories of means of identification have been specifically elevated by Congress gives victims of data breaches of those categories of data a good argument that they have been harmed. These categories are broad and encompass much of the personal data plaintiffs allege have been exposed.\textsuperscript{180} Therefore, on balance, the Courts should relax the showing of harm required of victims of data breaches.

The fact that Congress has passed an identity-fraud statute specifying certain means of identification as worthy of the protection of criminal law should be “instructive” in standing decisions.\textsuperscript{181} Where one of these means of identification has been seriously compromised, courts should grant standing to the victims. Serious compromises include hacking and exposures in which unauthorized people gain access to the means of identification. The potential for harm when one of the specified means of identification is exposed should be sufficient. Moreover, Courts should follow the Seventh Circuit in \textit{Lewert} and give standing to holders of credit and debit cards that have had their data compromised, regardless of whether the particular plaintiff has had fraudulent charges placed on her account.\textsuperscript{182} As the court recognized in \textit{Lewert}, the information on a credit card can be used to obtain other forms of credit using the victim’s identification.\textsuperscript{183}

This elevation by Congress, plus the experience of victims of identity fraud, should lead courts to reject the suggestion of the Second Circuit in \textit{McMorris} that purchasing a credit monitoring service after a breach constitutes manufactured standing.\textsuperscript{184} Identity thieves may wait before using the stolen identities to cool off the trail that may lead to them. Identity thieves can also apply for credit using the victim’s credentials and a different address. Without credit monitoring, the victim may learn of the harm only

\textsuperscript{178} See, e.g., Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 624 (7th Cir. 2020) (alleging violation of the Illinois’s Biometric Information Privacy Act for a data breach that exposed biometric information); Santana v. Take-Two Interactive Software, Inc., 717 Fed. App’x 12, 15-17 (2d Cir. 2017) (same).

\textsuperscript{179} See \textit{McMorris} v. Carlos Lopez & Assocs., 995 F.3d 295, 302 (2d Cir. 2021) (noting that some types of data, like dates of birth and social security numbers, give rise to a lifelong risk of identity theft, while other types of data, like credit card numbers, pose less of an ongoing risk because they can be canceled).

\textsuperscript{180} See supra Part I.


\textsuperscript{182} \textit{Lewert} v. P.F. Chang’s China Bistro, Inc., 819 F.3d 963, 966-67 (7th Cir. 2016).

\textsuperscript{183} Id.

\textsuperscript{184} \textit{McMorris}, 995 F.3d at 303 (2d Cir. 2021).
long after, when she applies for credit to buy a house or car. By then, she has suffered far more serious harm than the cost of credit monitoring. The fact that many companies that suffer breaches voluntarily pay for credit monitoring\textsuperscript{185} suggests that even the defendants in these cases recognize that the harm suffered is real. Thus, paying the cost of credit monitoring is preferable to the cost of more serious harms. Granting standing in cases where the only damage so far is the cost of credit monitoring will encourage companies that suffer data breaches to pay for monitoring and thus eliminate the easily quantifiable harm that victims suffer. This may have the same effect on reducing lawsuits as deciding that plaintiffs lack standing.

2. Civil Enforcement

The seriousness with which Congress takes hacking is reflected in authorized enforcement powers. That the Federal Trade Commission can take enforcement action against companies who have “fail[ed] to maintain security for sensitive consumer information” is another indication that the government takes data exposure harms seriously.\textsuperscript{186} Subjecting companies to liability for adequately protecting consumer data demonstrates Congress's view that this failure is a harm worth recognizing.

The FTC uses this power to act.\textsuperscript{187} But as even the FTC has acknowledged, “enforcement of the FTC Act alone may not be enough to protect consumers,” in part because the agency lacks the authority to seek


\textsuperscript{186} Privacy and Security Enforcement, FED. TRADE COMM’N, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement [https://perma.cc/N24P-XWHV] (last visited Sept. 27, 2023); see also 15 U.S.C. § 45 (prohibiting “unfair or deceptive acts or practices in or affecting commerce”). This prohibition has been the basis for enforcement actions against companies with lax data practices. See, e.g., Complaint at 6, In the Matter of Chegg, Inc. NO. C-4782 (Fed. Trade Comm’n 2023) (alleging that Chegg’s lax data security practices violated Section 5 of the FTC Act).

financial penalties for violations.\textsuperscript{188} Thus, criminal prosecution, civil enforcement, and plaintiffs who want to bring suit would together help to incentivize companies to invest in cybersecurity (because organizations would face increased civil liability in the event of a data breach) and deter unlawful conduct because would-be criminals would find less vulnerable organizations to hack into. Consumers primarily bear the burden of the numerous negative effects data breaches have on the economy, which eliminates some of the incentives for companies to guard systems carefully.\textsuperscript{189} Thus, giving consumers Article III standing in data breach cases may act as an additional push to companies to improve their data protection, making criminal hacking more difficult.\textsuperscript{190}

B. Attempted Identity Theft is Analogous to a Risk of Future Injury

Criminal law’s recognition of harm to victims of attempted identity theft is consistent with the reasoning that a future risk of injury flows from a data breach event, even one that has not yet led to identity theft. Section 1028(a)(3) prohibits possession of five or more means of identification with intent to use or distribute, which means that the crime is completed so long as the thief has both possession and intent, even if no victim has (yet) suffered theft. This statutory detail is informative in two ways. First, hackers who steal sensitive information with intent to use them maliciously have satisfied the elements of § 1028, and thus the analysis in Part A applies. Second, the victim does not have to have suffered identity theft for the actor to have engaged in a crime. This strengthens the analogy between data breaches and criminal hacking in thinking about both malicious conduct and harm to victims.

Harms from data breaches and attempted identity thefts are alike in part because their victims react similarly. Exposed plaintiffs in data breach cases have alleged, for example, purchasing credit monitoring services,\textsuperscript{191} investing time mitigating possible consequences, such as contacting the hacked

\begin{itemize}
\item \textsuperscript{189} See Gregory S. Gaglione Jr., The Equifax Data Breach: An Opportunity to Improve Consumer Protection and Cybersecurity Efforts in America, 67 BUFF. L. REV 1133, 1157 (2019) (“[T]he majority of these costs are not ultimately paid for by the entity that was breached. Rather, these costs are passed on to the consumer.”).
\item \textsuperscript{190} Id. at 1201.
\item \textsuperscript{191} Lewert v. P.F. Chang’s China Bistro, Inc., 819 F.3d 963, 965 (7th Cir. 2016) (“Based on that concern, he purchased a credit monitoring service to protect against identity theft, including against criminals using the stolen card’s data to open new credit or debit cards in his name. He spent $106.89 on the service.”).
\end{itemize}
company\textsuperscript{192} or canceling their credit cards,\textsuperscript{193} and experiencing stress and anguish.\textsuperscript{194} Experiencing emotional harm and investing time to protect against future theft are rational actions for victims of identity theft to take. While targets of attempted identity theft would not have to go through the same onerous process of actually mitigating the harms of theft, they may take analogously costly steps to guard against future attempted identity theft or spend money on expensive credit monitoring services. Vindicating exposed consumers in the data breach circuit split is analogous to vindicating victims of identity theft because taking preparatory action is the natural next step for anxious consumers responding to increased exposure and vulnerability. These measures are not, as some courts would hold, “manufactur[ing] standing simply by incur[ring] certain costs as a reasonable reaction to a risk of harm.”\textsuperscript{195} Rather, investing money and energy mitigating the possibility of harm down the road is a rational response to close calls.\textsuperscript{196}

C. Concentrated Criminal Attacks to One Individual Can Help to Conceptualize Small Harms to the Many

Criminal law’s usefulness to informing standing in the data breach context goes beyond the nature of the harms that it recognizes. Because data breach cases are generally class actions that aggregate a small amount of harm to many people, criminal law’s approach to harms of volume is also instructive. Injuries that seem small on the individual level can be large in the aggregate. In the privacy context, “the inconvenience of receiving an unwanted email or advertisement . . . adds up” on the scale of thousands of consumers.\textsuperscript{197} While someone could buy a credit-monitoring service for as little as $10 a month\textsuperscript{198} or spend a few minutes a day sorting through an influx of spam emails, these small harms distributed across large numbers of people in a data breach could

\textsuperscript{192} Kim v. McDonald’s USA, LLC, No. 21-cv-05287, 2022 WL 4482826, at *2 (N.D. Ill. Sep. 27, 2022).
\textsuperscript{193} Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1335 (11th Cir. 2021).
\textsuperscript{194} In re Practicefirst Data Breach Litig., No. 21-CV-00790, 2022 WL 354544, at *4 (W.D.N.Y. Feb. 2, 2022).
\textsuperscript{195} Legg v. Leaders Life Ins. Co., 574 F.Supp.3d 985, 994 (W.D. Okla. 2021) (quoting Clapper v. Amnesty Int’l, 568 U.S. 398, 416 (2013)) (internal quotation marks omitted); see also McMorris v. Carlos & Lopez Associates, LLC, 995 F.3d 295, 303 (2d Cir. 2021) (also quoting Clapper and concluding that protective steps are not alone to give rise to standing because plaintiffs are inflicting harm on themselves out of hypothetical fears of the future and thus manufacturing standing).
\textsuperscript{196} See Solove & Citron, supra note 133, at 766 (arguing that anxiety is a rational response to the increased risk of financial harm caused by a data breach).
justify an expensive damages claim.\textsuperscript{199} Or when thought about over a large
time frame, receiving a small volume of spam from numerous bad actors could
be just as harmful as one targeted attack.\textsuperscript{200} Time is valuable, and the energy
spent monitoring accounts and sorting through email spread over lots of
people over a long period of time could have been better spent.\textsuperscript{201} Recall that
this was, in part, the \textit{Webb} court’s justification for finding that time spent on
prophylactic measures led to a sufficiently concrete injury to confer
standing.\textsuperscript{202} It is true that no individual would take a big company to court
for a $10-per-month credit-monitoring service, but thousands of consumers
together have a legitimate class action claim. A big-picture view of all the
impacted consumers or a long-term view of one consumer exposed many
times suggests that data breaches, even when they do not actually lead to
identity theft or fraud (the major harms criminal law is worried about), do
cause exactly the kind of harm that courts have understood the CFAA to
vindicate.

D. \textit{Limitations of the Application of Criminal Law to Understanding Article III
Standing}

While the existence of hacking and identity theft statutes provides insight
into the harms experienced by victims and caused by perpetrators of data
breach events, the analogy has a limitation. Because prosecutors represent
the community, have discretion to bring cases, and must prove that the defendant
is guilty beyond a reasonable doubt, they are likely to charge with different
goals in mind than aggrieved consumers who want to hold companies
responsible for playing fast and loose with their personal data. While
prosecutors are aiming to promote community safety, general and specific
deterrence, rehabilitation and retribution, consumers are seeking an avenue
to redress less obvious injuries, like emotional harm and lost time and

\textsuperscript{199} See Citron \& Solove, supra note 197, at 816-17 (2022).
\textsuperscript{200} See id. at 816 (“When these harms happen to an individual repeatedly by different actors,
you become significantly more harmful. For example, receiving an unwanted email is a minor
inconvenience. Receiving hundreds of unwanted emails becomes a major imposition and
distraction.”). \textit{But see}, e.g., Czech \textit{v. Wall Street on Demand, Inc.}, 674 F. Supp. 2d 21102, 1115-16 (D.
Minn. 2009) (reasoning the plaintiff’s allegations of unwanted text messages were “too generalized
and abstract” to qualify as damage under the CFAA).
\textsuperscript{201} Solove \& Citron, supra note 133, at 756-61 (describing the legal basis for recognizing risk
and anxiety as cognizable harms).
\textsuperscript{202} \textit{Webb v. Injured Worker’s Pharmacy, LLC}, 72 F.4th 365, 377 (1st Cir. 2023) (“We join other
circuits in concluding that time spent responding to a data breach can constitute a concrete injury
sufficient to confer standing, at least when that time would otherwise have been put to profitable
use.”).
effort.\textsuperscript{203} Still, civil and criminal remedies have an important common goal: global data loss and theft reduction. The prosecutor charges the thief, hoping that doing so will deter him and others from trying to steal data down the road. A civil action against the data holder who suffered the leak might encourage data holders to improve security and in turn deter would-be criminals from pursuing the hacking business.

The goals of prosecutors and plaintiffs are not completely disconnected, but they are also not perfectly aligned. While a successful class action would provide symbolic as well as financial compensation for data exposure, a settlement (while not as symbolically powerful) provides similar financial benefits. On the other hand, prosecutors are ministers of justice devoted to furthering the goals of the criminal legal system and would likely not bring cases unless they believed they were in striking distance of proof beyond a reasonable doubt. Thus, there is a limit to how much the reasoning from Congress’s judgment and statutes in criminal law applies to recognizing injuries in the civil context.

Lastly, the most applicable reasoning from criminal law applies mostly to identity theft or attempted identity theft. While this analogy suggests that courts should take a more expansive approach to understanding harm where plaintiffs allege a real risk of identity theft because their exposed data is sufficiently sensitive, as in \textit{Webb},\textsuperscript{204} the analogy does not support the conclusion that the exposure of less sensitive data should give rise to standing. It is hard to imagine a prosecutor charging someone with hacking for stealing data that has no potential for identity theft or financial crime, although prosecutors are creative in finding ways to connect hacking of apparently low-stakes data to cognizable financial injuries.\textsuperscript{205}

On balance, the conduct Congress has chosen to criminalize, the legislative history of the federal identity theft statute, and a comparison of

\begin{footnotesize}
\textsuperscript{203} See \textit{Urness}, \textit{supra} note 115, at 1525 (“Plaintiffs who have not yet experienced identity theft resulting from a breach typically argue one of three injuries: risk of identity theft (a future injury), time and money spent on credit monitoring or other preventative measures (a present injury), or anxiety or emotional stress (a present injury).”).

\textsuperscript{204} See \textit{Webb}, 72 F.4th at 376 (considering the highly sensitive nature of the compromised data as a factor in determining the risk plaintiffs faced). Recall that in \textit{Webb}, one of the plaintiffs who had not alleged data misuse nonetheless had standing. \textit{Id.} at 374. The court reasoned that “the risk of future misuse may be heightened where the where the compromised data is particularly sensitive,” in this case, social security numbers, names, and dates of birth, among other data. \textit{Id.} at 376. In addition, that other plaintiffs had alleged actual misuse contributed to the court’s analysis that there was a real risk of future misuse. \textit{Id.} at 376.

\textsuperscript{205} See, e.g., \textit{United States v. Barrington}, 648 F.3d 1178, 1184-85 (2011) (describing, in prosecution under CFAA of hackers who changed their grades in a university database, prosecutors’ theory of the case that “the University incurred a loss of $137,000 due to lost tuition”).
\end{footnotesize}
harm precisely is a major challenge in privacy and cyberlaw. Harm is a gatekeeper because standing is a threshold issue. Demonstrating a cognizable injury in fact—or a harm—is a component of standing. But data breaches are a serious and growing problem with which courts must engage. In 2023 so far, the FTC received 5.7 million fraud and identity theft reports, and losses have cost Americans $10.2 billion in 2023 at the time of writing. Beyond these figures, there is the harder-to-quantify cost of hours on the phone, the time changing passwords, the emotional energy expended worrying about increased exposure, and the money invested in protective measures. These harms are not easily measured and may not be obviously “concrete” from a legal perspective, but where they are uncompensated by companies, the victims deserve a day in court.

Criminal law offers ideas for how to think about the harm from data breaches. That Congress criminalizes identity theft and computer fraud indicates that the legislators were concerned about the kinds of harms caused by data breaches when it enacted § 1028 and the CFAA. Attempted identity theft, which is also criminalized, has significant overlap with the harm to victims of data breaches who do not actually experience identity theft but may take protective measures in response. Recognizing standing in data breach cases would be one small step toward vindicating real but hard-to-define cyber harms.
