[*1]

Keach v BST & Co. CPAs, LLP
2021 NY Slip Op 50273(U)
Decided on March 30, 2021
Supreme Court, Albany County
Platkin, J.
Published by New York State Law Reporting Bureau pursuant to Judiciary Law § 431.
This opinion is uncorrected and will not be published in the printed Official Reports.

Decided on March 30, 2021

Supreme Court, Albany County

Elmer Robert Keach III, individually and on behalf of all others similarly situated, Plaintiff,

against

BST & Co. CPAs, LLP, Defendant.

ELEANOR MURRAY, on behalf of herself and all others similarly situated,Plaintiff,

against

COMMUNITY CARE PHYSICIANS, P.C., and BST & CO. CPAs, LLP,Defendants.

903580-20

Mason Lietz & Klinger LLP

Attorneys for Elmer Robert Keach III and Proposed Class

(Gary E. Mason and David K. Lietz, of counsel)

5101 Wisconsin Avenue, NW

Suite 305

Washington, DC 20016

Mason Lietz & Klinger LLP

Attorneys for Elmer Robert Keach III and Proposed Class (Gary M. Klinger, of counsel)

227 W. Monroe Street, Suite 2100

Chicago, IL 60630

Chaffin Luhana LLP

Attorneys for Elmer Robert Keach III and Proposed Class

(Roopal P. Luhana and Steven Cohn, of counsel)

600 Third Avenue, 12th Floor

New York, NY 10016

Weitz & Luxenborg, PC

Attorneys for Eleanor Murray and Proposed Class

(James J. Bilsborrow, of counsel)

700 Broadway

New York, NY 10003

Branstetter, Stranch & Jennings, PLLC

Attorneys for Eleanor Murray and Proposed Class

(J. Gerard Stranch, IV, Martin F. Schubert and Peter J. Jannace, of counsel)

223 Rosa L. Parks Avenue, Suite 200

Nashville, TN 37203

Turke & Strauss LLP

Attorneys for Eleanor Murray and Proposed Class

(Samuel Strauss and Austin Doan, of counsel)

613 Williamson Street, Suite 201

Madison, WI 53703

Cohen & Malad, LLP

Attorneys for Eleanor Murray and Proposed Class

(Lynn A. Toops and Lisa M. LaFornara, of counsel)

One Indiana Square, Suite 1400

Indianapolis, IN 46204

Gordon Rees Scully Mansukhani, LLP

Attorneys for BST & Co. CPAs, LLP

(Brian E. Middlebrook and John T. Mills, of counsel)

One Battery Park Plaza, 28th Floor

New York, NY 10004

Holland & Knight LLP

Attorneys for Community Care Physicians, P.C.

(Mark S. Melodia and Mark H. Francis, of counsel)

31 West 52nd Street, 14th Floor

New York, NY 10019

Richard M. Platkin, J.

The above-captioned actions arise from a December 2019 "ransomware" attack on the computer systems of BST & Co. CPAs, LLP ("BST"), an accounting and consulting firm. As a result of the data breach, hackers obtained access to BST's client data, which included the personal information of 170,000 current and former patients of Community Care Physicians, P.C. ("CCP"), a large medical practice.

On May 27, 2020, Elmer R. Keach III commenced Action No. 1 on behalf of himself and others similarly situated, seeking damages, restitution and injunctive relief from BST based on the firm's alleged failure to adequately safeguard the personal information of CCP members (*see* Action No. 1, NYSCEF Doc No. 1 ["Keach Compl"]). Eleanor Murray then commenced Action No. 2 on July 31, 2020, seeking similar relief from both BST and CCP on behalf of herself and others similarly situated (*see* Action No. 2, NYSCEF Doc No. 1 ["Murray Compl"]).

As both actions arise from the same facts and circumstances, the parties stipulated, "in the interest of simplifying motion practice," that BST and CCP would "jointly file a single motion to dismiss applicable to both the *Keach* Action and the *Murray* Action, with joint response and reply briefs to follow" (Action No. 1, NYSCEF Doc No. 13, p. 2). The instant motion practice ensued.

BACKGROUND

CCP is a large multi-specialty medical group with offices throughout the greater Capital District (*see* Keach Compl, ¶¶ 20-23; Murray Compl, ¶ 7). BST is an accounting, tax and advisory firm retained by CCP (*see* Keach Compl, ¶ 28; Murray Compl, ¶ 9).

Plaintiffs Keach and Murray are CCP patients and, in that connection, disclosed certain personal, financial and insurance information to the medical practice (*see* Keach Compl, ¶¶ 18, 25; Murray Compl, ¶¶ 5, 13-14). CCP, in turn, provided information concerning its current and former patients to BST in connection with a professional consulting engagement (*see* Keach Compl, ¶ 27; Murray Compl, ¶¶ 27-29).

On December 7, 2019, BST learned that a portion of its computer network had been infected with "ransomware" that prevented the firm from accessing certain electronically stored information (Keach Compl, ¶ 33).[FN1] BST retained a forensic investigations firm to determine the nature and scope of the data breach and eventually learned: a computer virus was active on BST's network from December 4, 2019 to December 7, 2019 (*see id*., ¶ 35); the virus was introduced by unknown individuals outside of BST who gained access to a portion of the network where client data, including member data provided by CCP, was hosted (*see id*., ¶ 36);[FN2] [*2]and, as a result of the foregoing data breach ("Data Breach"), certain personal information of current and former CCP patients "was accessed or acquired without authorization, including individuals' names, dates of birth, medical record numbers, medical billing codes, and insurance descriptions" (*id*., ¶ 37; *see* Murray Compl, ¶¶ 1-2, 28-29, 31-32).

On February 14, 2020, BST issued a "Notice of Data Privacy Event" to potentially affected individuals, including plaintiffs (*see* Keach Compl, ¶ 45 n 8; Murray Compl, ¶¶ 2 n 5, 36). The notice advised CCP members of the following:

> . . . On December 7, 2019, BST learned that part of its network was infected with a virus that prohibited access to its files. BST quickly restored its systems and engaged an industry-leading forensic investigation firm to determine the nature and scope of this incident. After a thorough analysis of all available forensic evidence, the investigation determined the virus was active on BST's network from December 4, 2019, to December 7, 2019. The virus was introduced by an unknown individual or individuals outside of BST who gained access to part of the network where certain client files are stored, including files from CCP.
>
> Because of the risk that data may have been accessed, acquired, or otherwise disclosed from its network without authorization due to the virus, BST reviewed the files in detail to determine what, if any, personal health information they contained. By February 5, 2020, in conjunction with CCP, BST confirmed the files contained some personal information for certain individuals and ascertained the addresses of these patients to communicate the security incident to them directly.
>
> . . . The investigation determined that, as a result of this incident, certain personal or protected health information for individuals may have been accessed or acquired without authorization, including individuals' names, dates of birth, medical record numbers, medical billing codes, and insurance descriptions. Patient medical records and Social Security numbers were not impacted by this incident.

> Although BST cannot confirm that any individual's personal information was actually accessed, or viewed without permission, BST is providing this notice out of an abundance of caution and to mitigate risk to individuals (https://web.archive.org/web/20210120161627/www.bstco.com/notice-of-data-privacy-event/ [web archive as of Jan. 20, 2021, last accessed Mar. 30, 2021 ("Privacy Event Notice")]).

In addition, BST offered "potentially impacted individuals access to complimentary credit monitoring services [for one year] as an added precaution and to mitigate risk" (*id*.; *see also* Keach Compl, ¶¶ 73-74).

After receiving the Privacy Event Notice, plaintiffs commenced suit against BST and CCP based on their alleged "collective failure" to prevent the Data Breach and safeguard the personal information that they entrusted to CCP, which included their names, dates of birth and [*3]medical billing and health insurance information (Murray Compl, ¶ 1).

Plaintiffs assert that they have been "significantly injured by the Data Breach" (*id*., ¶¶ 2-3). "Armed with the [compromised personal information], data thieves can commit a variety of crimes," including opening new financial accounts in the names of CCP members, taking out fraudulent loans, filing false tax returns, filing false medical claims, giving false information to police during an arrest, and obtaining bogus drivers' licenses (Keach Compl, ¶ 12).

Plaintiffs therefore contend that, "[a]s a result of the Ransomware Attack, [they] are exposed to a heightened and imminent risk of fraud and identity theft" (*id*., ¶ 13; *see* Murray Compl, ¶¶ 66-71). Plaintiffs further allege that they may incur out-of-pocket costs from the Data Breach, such as the cost of credit monitoring services, credit freezes, credit reports and other measures directed at detecting and preventing identity theft (*see* Keach Compl, ¶¶ 13, 84; Murray Compl, ¶¶ 75 [d], 77). Additionally, plaintiffs cite the time and expense associated with mitigation efforts, the loss of their "benefit of the bargain" with CCP, and the alleged diminution in value of their personal information (*see* Keach Compl, ¶¶ 84, 86-87; Murray Compl, ¶¶ 75, 78).

The Keach Complaint alleges four causes of action against BST: (1) negligence; (2) negligence *per se*; (3) violation of General Business Law ("GBL") § 349; and (4) breach of fiduciary duty. The Murray Complaint alleges seven causes of action: (1) negligence; (2)

breach of contract (CCP only); (3) trespass to chattels; (4) bailment (CCP only); (5) violation of GBL § 349; (6) unjust enrichment (CCP only); and (7) conversion (BST only).

Defendants now move for dismissal of the Keach and Murray complaints ("Complaints") on two grounds. First, defendants argue that plaintiffs did not, and cannot, allege that they have sustained an injury-in-fact from the Data Breach. According to defendants, "[p]laintiffs rely exclusively on the speculative possibility of harm that could occur in the future" (Action No. 1, NYSCEF Doc No. 19, p. 1). As a second, independent ground for dismissal, defendants contend that each cause of action alleged in the Complaints must be dismissed for pleading insufficiency.

Plaintiffs oppose the motion, except as to Keach's claims for negligence *per se* and breach of fiduciary duty (*see* Action No. 1, NYSCEF Doc No. 20 ["Opp Mem"], pp. 14, 19).

Remote oral argument on the motions was held on January 29, 2021, a certified copy of the argument transcript was provided to the Court on February 22, 2021 (*see* Action No. 1, NYSCEF Doc No. 30 ["Transcript"]), and this Consolidated Decision & Order follows.

ANALYSIS

"Whether a person seeking relief is a proper party to request an adjudication is an aspect of justiciability which, when challenged, must be considered at the outset of any litigation" (*Society of Plastics Indus. v County of Suffolk*, 77 NY2d 761, 769 [1991] [citation omitted]).

"On a defendant's motion to dismiss the complaint based upon the plaintiff's alleged lack of standing, the burden is on the moving defendant to establish, *prima facie*, the plaintiff's lack of standing as a matter of law" (*New York Community Bank v McClendon*, 138 AD3d 805, 806 [2d Dept 2016] [citations omitted]; *see* CPLR 3211 [a] [3]). The "motion will be defeated if the plaintiff's submissions raise a question of fact as to its standing" (*U.S. Bank N.A. v Clement*, 163 AD3d 742, 743 [2d Dept 2018] [internal quotation marks and citation omitted], *appeal dismissed and lv denied* 32 NY3d 1197 [2019]).

To have standing to sue, plaintiffs must allege the "existence of an injury in fact — an actual legal stake in the matter being adjudicated" that "ensures that [they have] some concrete interest in prosecuting the action" (*Society of Plastics*, 77 NY2d at 772-773). Each of

the named [*4]plaintiffs therefore must allege that he or she has suffered, or will suffer, an actual injury-in-fact by reason of the Data Breach (*see New York State Assn. of Nurse Anesthetists v Novello*, 2 NY3d 207, 211 [2004]; *see also Warth v Seldin*, 422 US 490, 502 [1975]; *Murray v Empire Ins. Co*., 175 AD2d 693, 695 [1st Dept 1991]; *Raske v Next Mgt., LLC*, 40 Misc 3d 1240[A], 2013 NY Slip Op 51514[U], *8 [Sup Ct, NY County 2013] [class representative must have "individual standing," which "means that the class representative must have an individual injury that is cognizable at law" (internal quotation marks and citation omitted)]).

"The injury in fact element must be based on more than conjecture or speculation" (*Matter of Animal Legal Defense Fund, Inc. v Aubertine*, 119 AD3d 1202, 1203 [3d Dept 2014] [citations omitted]; *see Matter of Brennan Ctr. for Justice at NYU Sch. of Law v New York State Bd. of Elections*, 159 AD3d 1299, 1301 [3d Dept 2018], *lv denied* 32 NY3d 912 [2019]), and the claimed injury cannot be "tenuous" or "ephemeral" (*Novello*, 2 NY3d at 214 [internal quotation marks and citation omitted]). Plaintiffs must allege an "'actual or imminent'" injury (*Matter of Association for a Better Long Is., Inc. v New York State Dept. of Envtl. Conservation*, 23 NY3d 1, 7 [2014], quoting *Lujan v Defenders of Wildlife*, 504 US 555, 564 [1992]) — one that is "impending" rather than "speculative" (*Whalen v Michaels Stores, Inc*., 689 Fed Appx 89, 90 [2d Cir 2017] [internal quotation marks and citation omitted]).

In evaluating whether plaintiffs in a data breach case have alleged an actual injury or the imminent prospect thereof, the New York courts have looked to five principal factors: (1) the type of personal information that was compromised; (2) whether hackers were involved in the data breach or personal information otherwise was targeted; (3) whether personal information was exfiltrated, published and/or otherwise disseminated; (4) whether there have been any incidents of, or attempts at, identity theft or fraud using the compromised personal information; and (5) the length of time that has passed since the data breach without incidents of identity theft or fraud (*see Smahaj v Retrieval-Masters Creditors Bur., Inc.*, 69 Misc 3d 597, 602-604 [Sup Ct, Westchester County 2020]; *Lynch v Johnson*, 2018 NY Slip Op 32962[U], *3-4 [Sup Ct, NY County 2018]; *Manning v Pioneer Sav. Bank*, 56 Misc 3d 790, 796-797 [Sup Ct, Rensselaer County 2016]).

The first factor looks to the type of personal information that was compromised and the extent to which the disclosure of such information renders individuals susceptible to identity

theft or fraud. The personal information at issue here consists of names, dates of birth, medical record numbers, medical billing codes and health insurance descriptions (*see* Keach Compl, ¶ 37; Murray Compl, ¶ 2; *see also* Privacy Event Notice).

While the foregoing collection of information about an individual certainly can be misused, particularly in connection with medical identity theft or other healthcare fraud (*see* Keach Compl, ¶ 67; Murray Compl, ¶¶ 40, 66-70), the instant cases are unlike those involving the disclosure of social security numbers or financial account information (*see Smahaj*, 69 Misc 3d at 599 ["names, dates of birth, social security numbers, and other information so that (collection agency) could collect on (plaintiff's) debt"]; *Manning*, 56 Misc 3d at 791 ["customers' names, Social Security numbers, street addresses, and some account and debit card numbers"]).

As plaintiffs recognize, the disclosure of social security numbers leaves individuals at a considerably greater risk of identity theft or fraud (*see* Keach Compl, ¶¶ 64-65), and the same is true of information concerning active financial accounts. The instant cases also differ from *Lynch*, where the compromised personal information belonged to New York Police Department officers, who are subject to heightened risks by reason of their official position (*see Lynch*, 2018 [*5]NY Slip Op 32962[U], *4 ["(i)n light of the risks faced daily by police officers, the dissemination of their personal information presents more risk"]).

The second factor looks to whether computer hackers were involved in the data breach or personal information otherwise was targeted. In this regard, case law recognizes that the involvement of computer hackers "creates an inference of malicious intent to steal private information, supporting an increased risk of identity theft" (*Smahaj*, 69 Misc 3d at 599, 601; *see Sackin v TransPerfect Global, Inc.*, 278 F Supp 3d 739, 747 [SD NY 2017] [distinguishing authorities involving "plaintiffs (who) did not allege or could not show that obtaining their (information) was the motivation for the theft"]; *cf. Manning*, 56 Misc 3d at 791 [laptop computer stolen from vehicle contained personal and banking information of customers]).

Plaintiffs specifically allege that the attack on BST's computer systems "was the work of the notorious Maze ransomware ring" (Keach Compl, ¶ 40; *see also id.*, ¶¶ 41-45). On the other hand, the Complaints repeatedly characterize the Data Breach as a "ransomware attack" (*id.*, ¶¶ 4-6, 33, 42; Murray Compl, ¶¶ 29, 45, 72), which, by plaintiffs' own definition, "is a type of malicious software that blocks access to a computer system or data, usually by

encrypting it, until the victim pays a fee to the attacker" (Keach Compl, ¶ 32). Thus, while ransomware deprives the victim of access to electronically stored information, the information itself ordinarily is not the object of the hackers' attack. Nonetheless, plaintiffs do allege that "the Maze ransomware gang has been known to extort businesses by publicly posting breached data on the Internet — and threatening full dumps of stolen data if the ring's 'customers' don't pay for their files to be unencrypted" (*id*., ¶ 41).

The third factor looks to whether the compromised personal information was exfiltrated, published and/or otherwise disseminated (*see Smahaj*, 69 Misc 3d at 599 ["Plaintiff alleges that the hackers attempted to 'place a batch of 200,000 payment card numbers for sale on a popular Darknet Market.' Plaintiff claims that due to the data breach, it is likely that she and other class members' private information 'will or has been disclosed already on the Darknet,' though there is 'uncertainty as to the nature and extent' of the information that was compromised."]).

Here, plaintiffs allege that their personal information was "stolen" (Keach Compl, ¶ 46; Murray Compl, ¶¶ 28, 40), citing the Maze ransomware gang's history of "extort[ing] businesses by publicly posting breached data on the Internet — and threatening full dumps of stolen data if the ring's 'customers' don't pay for their files to be unencrypted" (Keach Compl, ¶ 41). Relatedly, the Complaints cite a Florida data breach incident where hackers publicly released a portion of the stolen data as part of their extortion scheme (*see id*., ¶ 57). Plaintiffs also allege that the "Maze ransomware gang published the Private Data online for all cyberthieves to access" (*id*., ¶ 45; *see also id*., ¶ 91 ["published by hackers in January (2020)"]), but the Complaints do not include any particulars concerning this alleged publication, only a vague and conclusory allegation (*see e.g.* Keach Compl, ¶¶ 45-46, 91). **[FN3]**

Fourth, courts look to whether there have been any incidents of identity theft or fraud using the compromised personal information or any attempts to do so (*see Smahaj*, 69 Misc 3d at 603 ["the complaint fails to allege any actual suspicious activity that directly harmed plaintiff"]; *Manning*, 56 Misc 3d at 797 ["neither named plaintiff specifically identifies an actual or attempted identity theft or indicates any fraudulent charges"]). Plaintiffs do not allege any incidents of, or attempts at, identity theft or fraud using the compromised personal information of CCP members.

Finally, in cases like these, where there are no allegations of actual or attempted misuse of the compromised personal information, "a temporal component may factor into determining whether a threatened harm is sufficient for standing" (*Smahaj*, 69 Misc 3d at 601). In other words, "a lengthy passage of time without any suspicious activity weighs against finding an injury in fact" (*id*. at 602).

The intrusion into BST's computer systems occurred in early December 2019. Thus, nearly 16 months have passed without incidents of identity theft, fraud or similar misuse of the compromised personal information of CCP members (*cf. Smahaj*, 69 Misc 3d at 602 [almost 18 months since conclusion of data breach]; *Manning*, 56 Misc 3d at 791 [17.5 months]; *Jantzer v Elizabethtown Cmty. Hosp*., 2020 WL 2404764, *1, 2020 US Dist LEXIS 83207, *2 [ND NY, May 12, 2020, No. 8:19-cv-00791 (BKS/DJS)] [almost 19 months]). This lengthy period without incident counsels against finding injuries that are imminent or substantially likely to occur.[FN4]

Upon consideration of the foregoing factors, as well as the other arguments and contentions raised by the parties in their written submissions and at oral argument, the Court concludes that the two named plaintiffs, Keach and Murray, have not sufficiently alleged an injury-in-fact sustained from the Data Breach.

Even assuming that the personal information of plaintiffs, which did not include social security numbers or financial account information, was exfiltrated from BST's computer systems as part of the ransomware attack, plaintiffs have alleged no acts of identity theft, fraud or other suspicious activity involving their personal information. Nor have plaintiffs alleged any attempts to commit identity theft, fraud or other wrongdoing using their personal information.

Instead, plaintiffs are left to speculate about the prospect of future harms that may or may not come to pass (*see* Keach Compl, ¶¶ 77-84; Murray Compl, ¶¶ 71-75). As in *Smahaj*, plaintiffs rely on allegations of:

> (1) an increased risk of suffering from identity theft and fraud; (2) time, money, and other resources spent to mitigate against risks, both now and in the future, by cancelling credit cards, ability to open new bank accounts, reversing fraudulently imposed charges, and incurring high interest rates due to the inevitable decline in credit score when plaintiff [*6]and class members reasonably do not pay for items and services they did not purchase; and (3) the diminution of the value and/or loss

> of the benefits or products and services purchased directly or indirectly from defendants (*Smahaj*, 69 Misc 3d at 599-600).

But the passage of a lengthy period following the Data Breach with no suspicious activity weighs heavily against finding that the injuries claimed by the named plaintiffs are imminent or substantially likely to occur (*see id*. at 602-603).[FN5]

"Amorphous allegations of potential future injury do not suffice" (*Lynch*, 2018 NY Slip Op 32962[U], *3), and plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending" (*Jantzer*, 2020 WL 2404764, *6, 2020 US Dist LEXIS, *13-14 [internal quotation marks and citations omitted]; *see Clapper v Amnesty Intl. USA*, 568 US 398, 415-416 [2013]; *Whalen*, 689 Fed Appx at 90-91; *see also Caronia v Philip Morris USA, Inc.*, 22 NY3d 439, 446 [2013]). Thus, "[w]hile injury [from the Data Breach] is possible, as it was in [*Smahaj*, *Lynch* and *Manning*], it remains only a risk, too speculative to constitute injury" (*Lynch*, 2018 NY Slip Op 32962[U], *4).

As well articulated by the *Jantzer* Court in dismissing a similar data breach case against a healthcare institution:

> Those who are entrusted with details about an individual's health care should guard against even the inadvertent disclosure of that confidential information and those duties were allegedly breached in this case when hackers secured access to confidential health care information through a cyberattack. Nonetheless, while legal remedies may be pursued by those who were injured, the law only allows for the pursuit of . . . claims . . . only by those who have standing based on an alleged legally compensable injury. The Court finds the harm of increased risk of future identity fraud too speculative to support standing in this case (*Jantzer*, 2020 WL 2404764, *5, 2020 US Dist LEXIS, *12 [internal quotation marks and citation omitted]).

The Court therefore concludes that the named plaintiffs have failed to allege particularized and concrete injuries that are impending, imminent or substantially likely to occur (*see Smahaj*, 69 Misc 3d at 602-603; *Lynch*, 2018 NY Slip Op 32962[U], *4; *Manning*, 56 Misc 3d at 797; *see also Whalen*, 689 Fed Appx at 90-91; *Jantzer*, 2020 WL 2404764, *4-5, 2020 US Dist LEXIS, *11-12). For this reason, their Complaints must be dismissed.

In conclusion, the Court recognizes that the case law from outside of the New York State courts concerning the standing of data breach plaintiffs is far from uniform, and some federal courts and courts of other jurisdictions have found standing on facts somewhat similar to those presented here (*see* Opp Mem, pp. 5-6 & n 4; *see generally* Mitchell J. Surface, *Civil Procedure — Article III Cause-in-Fact Standing: Do Data Breach Victims Have Standing Before Compromised Data Is Misused?*, 43 Am J Trial Advoc 503 [2020]). The Court further [*7]recognizes that *Smahaj*, *Lynch* and *Manning* — decisions from courts of coequal jurisdiction — are not binding precedent (*see Matter of Todd*, 59 Misc 3d 852, 857 [Sup Ct, Erie County 2018]).

But the Court finds the multi-factor analysis taught by *Smahaj*, *Lynch* and *Manning* to be a sound approach to identifying whether the injuries alleged by data breach plaintiffs are "actual or imminent" (*Matter of Association for a Better Long Is.*, 23 NY3d at 7 [internal quotation marks and citation omitted]), rather than "based on . . . conjecture or speculation" (*Matter of Animal Legal Defense Fund*, 119 AD3d at 1203). Indeed, under New York law, the bulk of plaintiffs' claims do not even accrue and become legally enforceable until plaintiffs have sustained actual and ascertainable damages (*see Kronos, Inc. v AVX Corp.*, 81 NY2d 90, 96 [1993] ["It is the incurring of damage that engenders a legally cognizable right."]).

The ubiquitous nature of data breaches further counsels in favor of a cautious approach to standing. More than six years ago, a federal Judge addressing a data breach lawsuit observed: "There are only two types of companies left in the United States, according to data security experts: those that have been hacked and those that don't know they've been hacked" (*Storm v Paytime, Inc.*, 90 F Supp 3d 359, 360 [MD Pa 2015] [internal quotation marks and footnote omitted]). As illustrated by the reference sources copiously cited in plaintiffs' Complaints, the prevalence of data breaches has only increased since then.

CONCLUSION

For all of the foregoing reasons,[FN6] it is

ORDERED that defendants' motions to dismiss the complaints in Action Nos. 1 and 2 are granted; and it is further

ORDERED that the complaints in Action Nos. 1 and 2 are dismissed.

This constitutes the Consolidated Decision & Order of the Court, the original of which is being uploaded to NYSCEF for electronic entry by the Albany County Clerk. Upon such entry, counsel for defendant(s) shall promptly serve notice of entry on all parties entitled thereto.

Dated: Albany, New York

March 30, 2021

RICHARD M. PLATKIN

A.J.S.C.

Papers Considered:

Action 1: NYSCEF Doc Nos. 14-22, 30;

Action 2: NYSCEF Doc Nos. 12-20, 29.

Footnotes

Footnote 1:"A ransomware attack is a type of malicious software that blocks access to a computer system or data, usually by encrypting it, until the victim pays a fee to the attacker" (Keach Compl, ¶ 32).

Footnote 2: It later was reported that "the cyberattack on BST's computers like[ly] was the work of the notorious Maze ransomware ring" (Keach Compl, ¶ 40). "In recent years, the Maze ransomware gang has gained notoriety for 'shaming' victims by exfiltrating and publishing organizations' sensitive data. In particular, the Maze ransomware gang has been known to extort businesses by publicly posting breached data on the Internet — and threatening full dumps of stolen data if the ring's 'customers' don't pay for their files to be unencrypted" (*id*., ¶ 41). "BST was among 25 victims listed by the cybercrime ring on its

website, according to news reports" (*id*., ¶ 42).

Footnote 3: At oral argument, plaintiffs pressed the claim that the Maze ransomware gang exfiltrated CCP members' personal information from BST's computer systems and then published a *portion* of this data on the Internet in furtherance of an extortion scheme (*see* Transcript, pp. 12-14), in a manner similar to the Florida incident cited in the Keach Complaint (*see* ¶ 57). Even crediting the truth of this assertion, however, there is no allegation that the personal information of Keach and Murray, the two named plaintiffs, actually was published on the Internet (*see Raske*, 2013 NY Slip Op 51514[U], *8 [collecting authorities]).

Footnote 4: In a factually similar case, a Florida federal court observed that the provision of free credit monitoring to those potentially affected by a data breach, as was done here, further "lessen[s] risks of imminent injury" (*Stapleton on behalf of C.P. v Tampa Bay Surgery Ctr., Inc.*, 2017 WL 3732102, *3, 2017 US Dist LEXIS 139661, *6 [MD Fla, Aug. 30, 2017, No. 8:17-cv-1540-T-30AEP, Moody, Jr., J.]).

Footnote 5: The Court rejects plaintiffs' attempt to read the temporal component from the term "imminent" (*see* Transcript, pp. 33-35; *cf*. Black's Law Dictionary [11th ed 2019], imminent [defining "imminent" as "threatening to occur immediately," "dangerously impending" or "(a)bout to take place"]).

Footnote 6: The Court has considered the remaining arguments and contentions advanced by plaintiffs in support of standing (*see* Opp Mem, pp. 8-10), but finds them unpersuasive. And given the conclusion that plaintiffs lack standing, the Court has no occasion to address defendants' challenges to the legal sufficiency of the causes of action alleged in the Complaints.

Return to Decision List