Better Angry Than Afraid: The Case of Post Data Breach Emotions on Customer Engagement

John N. Angelis, Rajendran S. Murthy, Tanya Beaulieu, and Joseph C. Miller

***Abstract*—Extant research on data breach events primarily focus on the information technology lapses and delayed financial outcomes with less emphasis on the behavior of consumers. Essentially, current research prioritizes the *"what"* of data breaches, largely ignoring the question of "why." Our research seeks to fill a gap in the research design of prior studies on data breaches and customer behaviors by considering the customer emotions of anger *and* fear. While prior research has focused on anger due to its contagious nature, our results demonstrate that fear is the most influential emotion leading to changed behavior and/or lower revisit intentions. This article employs text and sentiment analysis of consumer responses to a data breach event to determine emotional response and revisit intentions. We find that angry customers may vent but will return with no meaningful change in their behavior. Unlike prior research, we also focus on fear and find that fearful customers retreat and disengage, behaving differently from angry customers. Managerial implications of this research illustrate the need to address fearful customers differently after a data breach to avoid reduced firm interactions and withdrawal behavior as opposed to merely reducing anger in the media as hitherto suggested.**

***Index Terms*—Customer relationship management, data analytics, data theft, hacking, information and telecommunication technologies, technology management, user–computer interaction.**

I. Introduction

AMERICAN consumers spend an increasing amount of time on the Internet with social media, digital streaming, and e-commerce taking center stage [1]. The US adult consumers spend an average of 145 min per day on social media, and that free and paid video streaming accounts for the second-largest traffic segment, with users spending between one and three hours a day [2]. In 2020, more than a quarter of online consumers streamed ten or more hours of video content every week [3]. Consumer retail spending has also transformed. The National Retail Federation projects retail growth to grow at 6%–8% in 2021, even after a 14% growth rate in 2021, accelerated by the aftermath of the Covid-19 pandemic, which outpaced slower growth in 2020 during the lockdowns [4].

As time spent online grows, hackers and data thieves have become increasingly sophisticated in their ability to target online customers and websites. The Identity Theft Resource Center, which tracks data breaches, recorded 11 762 data breach events that exposed over 15 billion records as of May 2020. Many of these data breaches were reported in large firms such as Home Depot, Target, Facebook, Sony, eBay, and Microsoft, which represent the giants in the retail, social networking, information technology, and digital media industries [5]. As attitudes toward work from home, distributed workforce, and online commerce gain strong traction due to the Covid-19 pandemic, issues relating to cybersecurity and data breaches are of paramount importance. For instance, T-Mobile announced its data breach of 40 million customers in August 2021 by blaming weakened security standards due to work from home policies [6].

Understandably, firms affected by data breaches suffer increased costs to shore up security, recompense customers, address public relations, and build defenses against future attacks. However, an equally important consequence of security breaches is customer churn. Studies note that customers are reticent to engage with breached firms for multiple reasons. For instance, Janakiraman *et al.* [7] find that retailers announcing a data breach suffered a 32.45% decrease in customer spending and a 20.28% decrease in web traffic to the retailer over the next seven months. Although some data breach-related costs are quantifiable, the cumulative negative effect of a breach and its resulting true costs remain nebulous, as it is difficult to accurately identify and attribute customer churn to the data breaches. Our research addresses the need to improve our understanding of customers who fail to reengage with the organization after a data breach.

Event studies using stock market data are a favored means of examining the impact of a data breach. Overall, these studies argue that data breaches result in losses for the firm due to negative media coverage in the short term, but also from lost customers in the long term [8]. However, these studies consider data breaches from a predominantly financial point of view, which limits the understanding of data breaches, specifically as it pertains to the subsequent behavior of consumers. These event study driven efforts prioritize the "what" of data breaches (what happens after a data breach), largely ignoring the question of "why" (why do consumers leave). Our research seeks to fill

Manuscript received 20 September 2021; revised 30 April 2022; accepted 10 June 2022. Date of publication 26 July 2022; date of current version 5 January 2024. Review of this manuscript was arranged by Department Editor S. Mäkinen. *(Corresponding author: John N. Angelis.)*

John N. Angelis is with the College of Business, University of Lynchburg, Lynchburg, VA 24501 USA (e-mail: angelis@lynchburg.edu).

Rajendran S. Murthy is with the Saunders College of Business, Rochester Institute of Technology, Rochester, NY 14623 USA (e-mail: rajsmurthy@saunders.rit.edu).

Tanya Beaulieu is with the Maine Business School, University of Maine, Orono, ME 04469 USA (e-mail: tanya.beaulieu@maine.edu).

Joseph C. Miller is with the College of Business, Saint Ambrose University, Davenport, IA 52803 USA (e-mail: millerjosephc@sau.edu).

This work involved human subjects or animals in its research. The author(s) confirm(s) that all human/animal subject research procedures and protocols are exempt from review board approval.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TEM.2022.3189599.

Digital Object Identifier 10.1109/TEM.2022.3189599

this gap in the literature by specifically seeking to answer the "why" of customer losses.

A few studies avoid the delayed effects of stock market changes by understanding revisit intentions of customers using a survey-based approach. For example, Chakraborty *et al.* [9] found that the severity of the data breach incident affected revisit intentions of seniors but not so for younger adults. Data breaches are emotional events for both those customers who are directly victimized (personal information leaked) and customers who are only indirectly affected (e.g., website down). Sharp [10] found that anger expressed actually increased over time for both categories of affected customers. Bachura *et al.* [11] found that the public went through a version of the Kubler-Ross stages of grief, reinforcing the notion that emotions played a much stronger role in data breaches. Additionally, Chatterjee *et al.* [12] investigated data breaches in physical retail environments and showed that customers who felt fearful had feelings of loss of control and increased uncertainty about the situation, which in turn reduced repurchase intentions. Therefore, research acknowledges the importance of understanding customer emotion after a data breach.

However, an issue with many of these research efforts is that they employ a scenario where the affected firm is preselected for the respondent. We believe that this approach suffers from two main limitations. First, sometimes a genericized firm is used (e.g., "Local Bank" or "Retail Co.") in a way that makes the scenario less likely to be associated with authentic customer emotions, experiences, or the power of the brand. Second, studies that used a specific firm in the research design did not take into account the involvement of the respondent with the industry domain. These designs largely ignore respondent relationship with the firm, especially when the respondent has little feeling toward the chosen website. For example, a college student may have very little involvement with a home improvement store or investment brokers but may have a stronger relationship with a video game console provider. Our research addresses this limitation by allowing respondents to pick their own favorite and frequently accessed website, thus ensuring respondents are primed to have a pre-existing emotional stake in uninterrupted service from the site.

A. Data Breaches As Service Failure

At its foundation, a data breach is the failure of the firm to deliver its service safely and effectively. Therefore, we adopt the Malhotra and Malhotra [13] view that data breaches represent a service failure incident; essentially a breach of contract with the customer. As Malhotra and Malhotra [13] show, this requires a coordinated, multidisciplinary response to reassure customers. To this end, the complexity of the phenomenon and the difficulties in quantifying churn require a service-dominant investigation of data breaches, i.e., a focus on customer reaction and subsequent reengagement. Yet, there is little research that addresses these aspects. Thus, the primary objective of this research is to add to the understanding of customer behavior post data breach so that firms may better manage their postbreach communication and reengagement efforts.

A recent development is the use of sentiment analysis to understand customer responses to data breach events. For example, Chatterjee *et al.* [12] use sentiment analysis and stock market data to understand effects of data breaches on customer behavior. In this article, we investigate the differential impact of emotions (fear and anger) instead of simply relying on a sentiment (positive, negative, neutral). In doing so, we show that these negative emotions have significantly different effects, and thus illustrate the need for firms to recognize how expressed emotions are linked to actual customer behavior. To capture these intricate and complex relationships, we employ a survey-based approach to collect data. We improve on previous research designs by allowing respondents to pick their favorite frequently used websites (separating paid and free sites), thus ensuring respondent involvement and emotional stake in getting uninterrupted service from this site. Finally, we consider the prebreach and postbreach sentiments through open ended text input from the respondents. We employ this design to investigate the following research question that guides our research:

RQ: To what extent do the emotions of customers drive their engagement with the website of a firm after a data breach?

In the following sections we begin by presenting the current literature on how consumers interact with online websites as well as respond to data breaches. Next, we detail our hypotheses and present our research design, followed by our method and results. We conclude with a discussion of the results alongside managerial implications, limitations, and potential paths for future research.

II. Literature Review

A data breach affects all stakeholders including the firm and its current and potential customers. The consequences span legal, monetary, and reputation domains as these breaches are essentially service failure incidents [13]. Consumers, in general, experience anxiety toward online security [14], and after a data breach they may arguably curtail future use of websites due to the risks involved [15]. Therefore, we organize our review of the literature around the nature of data breach violations, the relationship between customers and websites, and the responses to a data breach. To facilitate the subsequent review, we offer Table I that provides a quick reference to extant research that shapes our investigation.

Much of the extant literature is firm focused in the information technology domain with efforts to stop hackers, and employee policies and protocols for security as the highlight [16]. Firms must set up comprehensive strategies for dealing with possible data failures, whether from a public relations perspective [17] or from a service failure and recovery perspective [13]. Berezina *et al.* [18] indicate that such breaches result in an apparent loss of customer satisfaction, decreased chance of further purchases (revisit), and lower perceived service quality. All three are dimensions of the corporate reputation construct [19], which has been studied extensively and found to be significantly and negatively affected by data breaches. In the following sections,

TABLE I
RELEVANT LITERATURE

Author	Study	Relevant Findings
Wang & Huff (2007)	The study aims to explain buyer responses to data breaches as a violation of trust.	The perceived likelihood of repeated violation had significant effects on decline in trust, negative WOM and repurchase intentions. The magnitude of violation had no main effects, but interaction effects showed that *prior experience* with data breaches and *trust prior to the violation* have a significant and negative effect on buyer response.
Malhotra & Malhotra (2011)	This study associates breach reports with the decline in market value of firms using an event study.	The results show that firms suffer significant market value depreciation over a short as well as a long window of time. Due to the greater potential of customer backlash, negative publicity and liability risk, managers must view customer information breaches as service failures rather than as information system failures.
Sinana & Zafar (2016)	Investigate the financial impact with the reputational damage of data breaches with social media data.	Shareholders *do not* react negatively to data breach announcements even when the impact on reputation is statistically significant and negative.
Kim, Johnson, & Park (2017)	Study how crisis managers should deal with a data breach crisis.	While retailers used a full range of response strategies including denial, ingratiation, and regret, *news media outlets chose to report more on the advocate strategies such as scapegoat or excuse*.
Rasoulian, Grégoire, Legoux, & Sénécal (2017)	Study differentiates between cause of breach, crisis severity and apology intensity to better understand stakeholder mentalities post breach.	*Compensating consumers post breach and process improvement have an equal effect size on firm-idiosyncratic risk*. This research deviates from prior behavioral meta-analysis which found a difference between these approaches
Goode, Hoehle, Venkatesh, & Brown (2017)	Addresses methodological limitations in prior data breach and service failure literature by using longitudinal data.	Treats data breaches as service failure events. *Finds that customer repurchase intentions are negatively influenced when there is any discrepancy between expectations of compensation and actual experiences*.
Kashmiri, Nicol, & Hsu (2017)	Examines intra-industry spillover effects after a data breach.	*Data breaches do have a contagion effect*. In this study, the (Target) data breach was shown to result in negative abnormal returns for other retailers.
Martin, Borah, & Palmatier (2017)	Using a field study approach this research shows the effects of data vulnerability on consumer outcomes.	*Levels of violation and trust (pre and post) mediate the effects* of data vulnerabilities on outcomes post breach.
Confente, Siciliano, Gaudenzi, & Eickhoff (2019)	The goal of the study was to discover how reputational dimensions changed after data three types of data breach events.	Prior to breaches, consumers typically discuss the perceived quality dimension of a firm's offerings. After all three types of data breaches, consumers also pay attention to customer orientation and corporate performance dimensions of corporate reputation.
Li & Stacks (2017).	This article investigated the consumer response mechanism in a service failure context using a survey. Study proposes and tests a model with emotive antecedents, a mediation process.	Results show that anger and dissatisfaction were emotive antecedents that lead to consumers' exit, voice, and revenge responses.
Van Schaik, Jeske, Onibokun, Coventry, Jansen, & Kusev (2017)	Examines security hazards on the Internet and consumer perceptions across two countries.	Need for control is a significant predictor of precautionary behavior.
Gwebu, Wang, and Wang (2018)	Study investigates response strategies that can mitigate the negative financial impact of a breach on lower-reputation firms	Response strategies are found to matter less for high-reputation firms. More nuanced strategies built on prior attitude and reputation of the firms are needed for managing data breaches.
Janakiraman, Lim, & Rishika (2018)	Examine the role of customer data vulnerability as the behavioral mechanism that drives customer behavior subsequent to a breach.	Retail consumers affected by data breach decrease their spending, however, they simply migrate from breached channels to alternate channels. Consumers with higher retailer patronage are *less likely* to change behavior.
Zou, Mhaidli, McCall, & Schaub (2018)	Study examines one of the largest breaches in U.S history – the Equifax, breach in 2017 to understand consumer perceptions of risk and protective measures undertaken.	Findings show that consumers' mental models of credit agencies are incomplete and partially inaccurate. Consumers basically have asymmetric information and are not well informed of the impact of the data breach.
Choi, Park, & Jung (2018)	Study examines privacy fatigue from the management of online personal data.	The increasing difficulty in managing one's online personal data leads to individuals feeling a loss of control resulting in privacy fatigue. Privacy fatigue has a stronger impact on privacy behavior than privacy concerns.
Kesgin & Murthy (2019)	Study explores interplay between prior experience and loyalty intensions.	Prior experience does not appear to yield better outcomes, however it does predict revisit intentions.
Chatterjee, Gao, Sarkar, & Uzmanoglu (2019)	Study differentiates between fearful and angry consumer reactions to the scope of a data breach (# affected).	Fear makes consumers less likely to purchase from the affected retailer the larger the scope of the breach. An increase in anger causes consumers to become scope insensitive but does not affect repurchase intentions.
Angelis & Miller (2021)	Study uses a survey to investigate consumer response to website breaches based on the customer perception of the nature of the breach being individualized to the victim.	When the breach is individualized, consumers tend to place more blame upon themselves for the incident and the thieves, and place less upon the retailer. When it is not individualized, the consumer places blame on the retailer, and pay begrudging respect for the skills of the data thief.
Xiaojuan, Zhang, Angelopoulos, Davison & Janse (2022)	Study addresses the relationships among security breaches, organization response strategy as well as consumers' threat and coping appraisal.	The chosen post breach response strategy of an organization can lead to significantly different consumers' reactions. Consumer concerns tend to be short-lived even if data breach announcements have a negative impact on consumers' perceived risk. Overall, consumer concerns are mitigated by corporate reputation.

we review important concepts that showcase customer privacy and data breach concerns.

A. Privacy Fatigue and Privacy Paradox

Customers using websites are required to disclose information in order to realize the full benefits of the website. For example, customers seek and gain social currency by leaving detailed reviews on locations they visit on vacation [20], but this involves giving up detailed information about one's location, plans, and preferences. While data is a valuable asset, the more data the firm has on the consumer, the more vulnerability they face in a security breach [13]. This tension is referred to as privacy fatigue [20], whereby users become emotionally drained and cynical about data privacy. For example, the decision to continue to use social networking sites is a complex framework involving perceptions of privacy risks, trusting beliefs, network characteristics, and gratification from its use [21]. Users may become overwhelmed with information or complacent regarding security, both of which result in no change in the future use of a website [22], [23]. Privacy fatigue is a likely explanation for consumer inaction in the face of data breaches and perhaps for the confusing guidance from the firm itself, e.g., [24].

Another perspective of this tradeoff is the so-called privacy paradox, where customers express large concerns about internet privacy but continue to engage in behavior inconsistent with this concern. However, research reports mixed findings on this front. For example, Hoffmann *et al.* [25] and Kokolakis [26] found support, but Mothersbaugh *et al.* [27] found that it differs based on the type of data shared on the site. It is therefore possible that some websites are immune to some of the privacy paradox [28]. However, many free websites and social networks in particular require deeper disclosure than nonsocial networks. So, while customers may want to protect their data, the websites are designed to encourage sharing in a manner [29] that overcomes this privacy paradox. It is entirely possible that sites with better corporate reputations are less at risk from the outcomes of data breaches [19], and thus are able to bypass struggle of the privacy paradox. Therefore, the type of information shared and type of website that may be breached, are both of importance in these investigations.

B. Customer Responses to Data Breaches

Several studies note that data breaches lead to increased cynicism, and erode trust and commitment to the organization. They state that this ultimately leads to decreased interactions with the organization [30]. Several studies focus on the cognitive processing of individuals e.g., [31]–[34] to shed more light on this phenomenon. Specifically, coping strategies and disengagement behaviors are identified in postbreach incidents. Disengagement relates to removing personal information, providing false information, leaving the website, or deleting the account [35], p. 44. The general notion put forward in the literature is that disengagement is a stressor avoidance mechanism. Lee and Lee [36] refer to these actions as "retreative behavior." Coping strategies are more nuanced and may be divided into problem-focused coping (PFC) and emotion-focused coping (EFC) [37]. PFC is the "adoption of protective measures or cost–benefit analysis" to cope with security threats and addresses the action component of reacting to a security breach. EFC, on the other hand, represents the strategies used to control or dampen the emotions aroused by a stressful situation [38]. EFC can be further divided into inward-coping strategies such as distancing, denial, and wishful thinking, and outward-coping strategies such as seeking emotional support and venting [37].

Bagozzi [39] examines emotional responses as a coping mechanism. He states that the initial appraisal process is followed by an emotional reaction, which in turn then triggers a coping response. In the case of a data breach, the process begins with an appraisal which consists of an assessment of the data breach—i.e., what was stolen and what is at stake. This is followed by an emotional reaction (fear, anger, etc.), which then drives the coping response. Similarly, appraisal theory notes that different emotional responses will lead to different actions [40]. More specifically, it reveals that inward-EFC impedes PFC, whereas outward-EFC facilitates PFC [37]. Therefore, the results of these internal processes determine the ultimate action taken by an individual.

Understandably, emotions play a key role in reaction to a security breach and subsequent action, e.g., [41]. However, unlike core affect, emotions have different contagion and action effects. For example, Fan *et al.* [42] showed anger is more easily passed on from user to user than sadness. Notably, Chatterjee *et al.* [12] investigated the differential role of fear and anger in data breaches, and found that both fear and anger were affected by scope of the data breach and lead to different outcomes.

However, we have a limited understanding of actions that victims take after a security breach as some of these actions may be inaction and disengagement. These responses are abstracted from the firm's vantage point. A small number of studies connect consequences of data breaches to changes in consumer behavior postbreach. Mamonov and Koufaris [30] find that data breaches lead to lower trust and commitment and higher cynicism toward the provider thus increasing the likelihood of leaving the provider. The severity of the breach also influences intention with more severe breaches leading to increased likelihood of leaving, especially for those who are risk averse [43]. Due to the paucity of studies surrounding the affective component of data breaches, our article analyzes the emotional reaction and subsequent action of customers after a data breach.

III. Hypotheses and Research Model

Current literature fails to achieve consensus on the behavioral outcomes of a data breach, with some studies indicating abandonment while other studies indicating little to no change in the customer base [7], e.g., [12], [44], [45]. We propose that these differences are due to two limitations in current research. First, very few studies consider the emotional reaction of the consumer to a data breach. Second, of the studies that did consider emotions, few unpack the general concept of "emotion" into specific emotions and instead rely on the dichotomous

(positive versus negative) nature of consumer voice. In this article, we deconstruct the emotions expressed by consumers and examine the differences between anger and fear reactions to a security breach and examine it alongside subsequent customer behavior.

Unlike prior studies which use attitudinal measures as control variables for the website under consideration, we instructed participants to select their own favorite websites as the stimuli. Therefore, we ensure a positive disposition and high involvement with the website under consideration. Similar to prior studies our research design employs a scenario-based approach by first announcing the data breach and subsequently obtaining post-breach reactions. Therefore, we focus on how customers react emotionally to a data breach and how variations in emotions expressed lead to different behavioral outcomes.

Customers who feel more positively about the site are less likely to change their behavior after the breach. In simpler terms, these customers will likely continue their patronage despite a data breach incident. Such loyalty is of great value to a site for recovery and to better manage customer retention efforts post-breach. This aspect of loyalty is an oft-researched component of several data breach studies (e.g., the effects of communal versus exchange relationship with business in Gao *et al.*, [45]). However, research shows that this result is not always to be expected [44], and that context matters. For example, research has shown that retail customers who spend larger amounts at the website are more forgiving of the firm postbreach, and hotel patrons who have a long-term relationship with the brand appear to be more forgiving [46], [47] than others. Therefore, while prevailing disposition does play a role, the behavior of the customer after the data breach may not always be predicted on that basis. Understandably, this requires further scrutiny and leads to our first hypothesis.

Hypothesis 1: Consumers with favorable sentiment toward the website pre data breach are less likely to change their revisit behavior post data breach.

All data breaches will raise concerns, especially, in our context of a "favorite website" being breached. Reactions to these breaches could lead to negative emotional expressions at several levels of fear and/or anger. However, it is unclear as to whether these negative emotions manifest as changed behavior. Drawing from the literature on EFC and PFC, and guided by appraisal theory, we posit that customers may turn outward toward social media, customer service channels, and electronic word of mouth to express how upset and/or frustrated they might be, while other customers may turn inward with feelings of fear, guilt, and shame.

As discussed, research has established the need to study fear and anger when dealing with risk and uncertainty in outcomes. However, it does suggest that consumers felt more in control when events lead to anger compared to events that elicit fear. In response to a stressful situation, emotion-focused coping is used to control or dismiss the emotional reaction to a stressful situation [48]. Different outcomes will result depending on the emotional focused coping skill enacted by an individual [49].

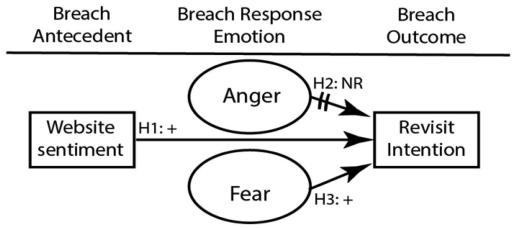


Fig. 1. Conceptual model of sentiment/emotional responses to data breaches.

Customers who experience anger are using an emotionally outward coping strategy. Outward coping strategies include venting emotions and emotional support seeking. Literature shows that these outward coping strategies lead to action, but in the context of a favorite website, we argue that the action expressed by angry customers will be in the form of venting, not changes in revisit behavior. Li and Stacks [50] verify that anger and dissatisfaction indicate that a customer may exit, complain, or even take a measure of revenge when reacting to a service failure. It is likely that customers who express anger may exaggerate the extent of their emotion with the company for their lost/stolen information in order to gain a better settlement or to gain sympathy from their online friends, even though they have no actual intent of leaving the company. Having vented their anger, we propose that these customers will return and continue their use of the website.

Hypothesis 2: Anger postbreach will not be associated with changes in revisit behavior.

Data breaches undoubtedly elicit vulnerability in some customers [51], which may lead to fear. Fear emotion draws some of the blame for the breach inward toward themselves, and consumers may experience denial or may be frozen from taking any action. This emotional response does not lead to venting, or perhaps even discussing the breach with close friends or family. Fearful customers may choose to enact an "adaptive withdrawal." In other words, customers may take certain actions to reduce their stress and vulnerability [52]. This fear may lead to defensive or protective behaviors or perhaps a sort of paralysis that ultimately leads to withdrawal and avoidance.

Behaviorally, when consumers feel fear they are more likely to engage in actions that minimize uncertainty [48], [53]. Fear elicits powerful brain chemicals and the triggering of the amygdala which is associated with memory. Research shows that fear can result in actions which might be categorized as a "better safe than sorry" approach [54]. In terms of actions, this may manifest as customers leaving the website, or make some defensive changes such as deleting a credit card or updating a password. These inward coping skills help quell the fear by focusing more on the cause of the security breach [37]. We propose then that these fearful customers will take actions that disconnect themselves from the website.

Hypothesis 3: Fear postbreach is associated with increased changes in revisit behavior.

See Fig. 1 for our research model.

TABLE II
DEMOGRAPHICS

Gender	Male	44%
	Female	56%
Ethnicity	Asian	14%
	African American	7%
	Hispanic	5%
	White	68%
	Other	6%
Age	18–20	44%
	21–22	28%
	23–25	11%
	26–40	8%
	>41	9%

Note: For reference, U.S. Census reports that graduating students from U.S educational institutions are 61.2% white non-Hispanic, 13.6% Hispanic, 12.3% black, and 11.2% Asian. (https://www.census.gov/newsroom/press-releases/2018/school-enrollment.html).

IV. METHOD

A. Data Collection

Our survey polled a convenience sample of 208 participants composed primarily of 2 undergraduate student bodies from the Northeast United States. The survey resulted in 150 usable responses included in the analyses. Participants were predominantly Caucasian (68%) with a mean age of 24 and all had some college education (>2 years). Participants self-reported gender with 44% identifying as male and 56% as female. Demographics are presented in Table II for reference. Participant demographics compare closely with the U.S census data as noted but underrepresent Hispanic and African American populations.

Participants were randomly allocated one of two survey prompts. The first asked them to select a favorite free website (e.g., social networks), and the second asked participants to select a favorite paid website (e.g., e-commerce sites). In both categories, participants were instructed to choose a site where they had a personal account (i.e., no guest only or nonlogged-in access). In both cases, participants were reminded to only select a website which they personally used frequently. The websites chosen by the participants included 71 free websites (e.g., Facebook, Instagram, and YouTube) and 78 paid websites (e.g., Netflix, Adobe, Hulu). The research instrument used was adapted from Angelis and Miller [55]. The instrument consisted of three main components. In the first component, participants were asked to first name their favorite site, then supply several single word attributes associated with the website in a free association type task. This was followed by an open-ended description as to why the website was their favorite website. We instructed the participant to select their favorite frequently used website, therefore we anticipate that the participant has a positive predisposition toward that website. The second component of the survey was designed as a distractor task. Participants were asked to caption a few memes provided to them at random. The purpose of the distraction was to ensure that the participant was engaged in an activity before being presented the data breach scenario. The third component presented the participant with a breaking-news type article describing a site data breach (inserted from the prior step). As before, participants were asked to choose five distinct words to describe their feelings about the data breach. Finally, we asked participants to respond to an open-ended question to ask participants what their future intent would be regarding their use of the website. Several surveys were opened but incomplete. We chose to delete incomplete surveys and after these deletions we were left with 150 completed and usable surveys ($N = 150$).

B. Measures

1) Pre- and Postbreach Sentiment: Data in the first component of the survey collected information on the participant feelings toward a favorite website of their choice. As a means of validation, the participant's sentiment toward the website was measured by evaluating the sentiment of the text used by the participant to describe their attitude toward, and use of, the website on a daily basis. This serves as a proxy to the well-established attitude toward a brand measure which uses semantic differentials such as (bad/good, useful/useless, etc.). The five words provided and the open-ended text in paragraph format served as the input for the sentiment expressed pre- and post data breach announcement manipulations. For example, regarding the prebreach sentiment, a participant noted the five words as "useful," "enjoyable," "quick," "easy," and "interesting" and provided the open-ended input as "…every time I log on to it, there's something interesting on the 'top' section. It also has a lot of funny articles that usually refresh my mind when I'm taking a break from work…" We first used the five-word description to calculate an average sentiment score and compared it with the sentiment expressed in the open-ended input. Prior to the data breach announcement, we found that the sentiment expressed in the five words and the sentiment expressed in the sentence to be strongly correlated ($r = .77$, $p < 0.05$). This consistency provided a form of validation for the use of this approach. We calculated the sentiment from the text provided by the participant after they were told of the data breach in a similar manner as a secondary validation. In the post data breach announcement stage, we found a similar correlation ($r = .81$, $p < 0.05$) indicating consistently robust results.

2) Emotion: Fear and Anger: In both cases, sentiment was scored on a word-by-word basis using the NRC lexicon manually. This was necessary as each word was given a polarity (magnitude of positive or negative sentiment) and then the score summed to form the overall sentiment and then averaged over the number of words provided by the respondent. A similar process was followed for extracting the emotive elements in the participant open ended text responses, but here the process was completed by using R and the *SentimentR* package to extract sentiment and emotions expressed. *SentimentR* was chosen over other packages because of its ability to handle valence shifters (e.g., very good, very bad) and amplifiers as opposed to simple dichotomous positive/negative assessments. Furthermore, *SentimentR* provides polarity measures that take into account the magnitude of positivity or negativity expressed as opposed to simple positive negative evaluations. The outputs provided data on the overall sentiment (adjusted for the length of the response) along with a measure of anger and fear as expressed in the open-ended text. The use of anger and fear in this context was

TABLE III
DESCRIPTIVE STATISTICS

	M	*SD*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
1. Paid/Unpaid	.53	.50							
2. Gender	1.11	.38	.02						
3. Preliminary sentiment	3.93	.59	−.09	−.03					
4. Post-breach sentiment	2.99	.85	−.11	−.08	−.20*				
5. Anger	.76	.70	−.10	.16*	−.04	−.02			
6. Fear	1.12	.88	−.05	.07	−.04	−.02	.289*		
7. Revisit Intention	1.67	.47	−.06	.04	.09	.04	−.09	−.16*	
8. Age	24.1	6.17	.44	.03	.11	.19	.01	.18	−.21

Note: $N = 150$, Education ($M = 3.78$, SD 1.41).

guided by prior research. While the lexicon does include other emotions such as surprise, disgust, joy and anticipation, these were less prevalent in the results and thus were not used in the research.

3) Validations of Sentiment Measures: Respondents were able to select their favorite site for this survey. Thus, we can be sure that all respondents have a positive relationship with the breached site and will at least feel inconvenienced when they are informed about the data breach. The mean preliminary sentiment toward the website supports this assumption ($M_{\text{pre}} = 3.93$). In addition, customers were not informed that the survey was about data breaches, so their response was expected to be genuine. To confirm the manipulation, we conducted a *t*-test to check if attitudes changed before and after being told of the data breach. Results indicated a significant difference verifying the manipulation and impact of being informed of a data breach ($M_{\text{pre}} = 3.93$, $M_{\text{post}} = 2.99$, $p < 0.01$, df $= 149$). Means, standard deviations, and correlations are presented in Table III.

V. RESULTS

Participants indicated how they would change their behavior as a result of the breach as part of the survey. Two authors reviewed all individual responses and classified each respondent into one of the following three categories:

1) those that will not return;
2) those that will return with significantly changed behavior;
3) those that will return without any change in behavior.

Disagreements were resolved through discussions by involving the other coauthors. Interjudge reliability was high (96%) supporting the consistency of the process. This step was necessary as our research is particularly focused on understanding the entire spectrum of customer behavior changes.

A. Changing Behavior

Our three-level classification allowed us to run two separate but reinforcing analyses. First, we ran a series of ANOVA's to understand the impact of pre- and postbreach sentiment and emotions expressed on revisit intention at the two levels (will return/will not return). This is closer to the operationalization in prior studies. In the second analyses we were able to use a logistic regression approach to investigate the change in behavior as the dependent variable of interest using the same predictors. This dual approach helps us more fairly cover respondents who indicated that they would stay on the site *but* make significant changes in behavior. For clarity we labelled these as defensive behaviors. This was particularly important in light of the fact that 101/150 participants planned to return as indicated by their response to the question (will revisit/will not revisit). Comparatively, when including defensive behavior, only 40/150 indicated that they would return with no changes, 61 revealed that they would change their behavior prior to returning, and the remaining 49 would simply not return. Indeed, this distinction may well be the missing explanation for inconsistent findings in prior research. It is easily argued that these changes in behavior can be significant and lead to long-term effects. For example, customers who remove their personal information and/or credit card may be worth significantly less to the website. Research has shown that saved payment information, perceived safety of the website, and trust in the site are all factors that influence online commerce positively [56]. Research on data breach in the retail realm confirms that customers lose trust and have anxiety and fear for future patronage of websites and services that have suffered breaches [57], [58]. We present the results of the analyses using revisit intentions for transparency along with potential explanations for this behavior. Throughout the testing of our hypotheses, we controlled for age, gender, and paid/unpaid classifications of the website.

B. Revisit Intention

We conducted several one-way ANOVAS to examine the role of the emotions expressed in the open-ended text with revisit intention (will return/will not return) as the variable of interest to test H1, H2, and H3. Our results indicate that only fear was significantly different ($F = 3.849$, df $= 1,148$, $p = .05$) between participants who intended to return and those who indicated that they would not return. Anger, on the other hand, was not significantly different ($F = 1.076$, df $= 1,148$, $p = .30$). Furthermore, there was no difference between the paid and unpaid sites. The control variables age and gender were also similarly insignificant. Taken together, these results show support for H2 and H3 but fail to support H1. We then moved to our second analysis to re-examine the hypotheses but to drill down by examining the customers who changed their behavior and those who chose not to return at all.

C. Defensive Behavior Changes

In order to investigate the changed behavior separately, we split the original dataset into two different subsets, one where participants indicated that they would revisit and others who

TABLE IV
CHANGED BEHAVIOR QUOTES FROM OPEN ENDED RESPONSES

Respondent	No Change in Behavior
25	It wouldn't affect me at all because I use my nickname as login and most of the information I put on their website is barely accurate. I also have nothing to hide so wouldn't care if the data does go public.
44	I would still use them, because all I needed to do was cancel a card
109	I would probably be using it in the future. It's a great service with no competition good enough.
Respondent	Change in Behavior
177	If there were a lot of changes to it, I would probably stop using it, or use it less frequently, and be very cautious when using it.
48	I would probably look toward using another online shopping service like eBay or the like.
86	I would be very mad if I lost all of my pictures and friends and probably wouldn't use it anymore if it had problems.
16	I would delete my Facebook account
92	(First of I thought this was real lol) But anyway i would remove my credit card information right away from the site.(My heart is beating a little fast as i write this words). I would delete my account write away. so in short NEVER!!!!

TABLE V
LOGISTIC REGRESSION WITH CHANGING BEHAVIOR AS DEPENDENT

	B	*S.E.*	*Wald*	*df*	*Sig.*	*Exp(B)*
Constant	−.85	1.47	.34	1	.56	.43
Preliminary Sentiment	.28	.33	.74	1	.39	1.32
Age	.01	.02	.04	1	.83	1.01
Gender 1 - Male	−.28	.40	.48	1	.49	.76
Paid/Unpaid 1 - Unpaid	.39	.38	1.10	1	.30	1.48
Anger	−.13	.60	.80	1	.64	.88
Fear	.67	.28	.22	1	.02	.88

Note: Dependent—Change behavior (N=101, M=1.74, SD=.440).
Exp(B) as odds ratio for corresponding variables reported for logistic regression. Logistic regression accurately predicts 74% of the cases at a .5 standard threshold.

would not revisit. For those who would revisit we added an indicator to show when (and if) participants would change their behavior prior to the revisit (e.g., remove credit card information, use without logging in, remove account but continue to use as a guest). It is important to note that the majority of actions listed are defensive, and many, if not most, are not necessarily useful or effective solutions. In order to get a sense of the comments and the variety of responses postbreach, we present a sample of these comments for reference in Table IV.

We chose to test our hypotheses using a logistic regression approach with changed behavior as the dependent variable with the preliminary sentiment, postbreach sentiment, anger, fear, and paid/unpaid status of the website as predictors. This model represents a more realistic, albeit pessimistic outlook of the damage done as the result of the data breach. Results presented in Table V confirm our prior findings that only Hypotheses 2 and 3 are supported. Fear remains the only significant predictor ($B = .665$, $p = 0.02$, Exp(B) = .876), lending further support for the need to focus on the fear, and not anger, as expressed by the customers. Fear greatly increases the potential for defensive measures, including deleting or canceling the accounts on the websites that were breached. The Hosmer and Lemeshow test chi-square of 4.704 with a $p = .789$ indicates that the model has adequate fit. The model accurately predicted 74% of the outcomes at a .5 threshold. Consistent with prior analyses, the paid/unpaid status of the website did not have any impact on the outcomes.

VI. DISCUSSION

The goal of our research was to bring together sentiment analysis and data breaches to help extend the current understanding of data breaches from the perspective of those affected. To address our research question, our analyses showed that preliminary positive sentiments are not necessarily associated with customer behavior postbreach. Instead, interpretation of the data breach leading to emotional response appears to be more important when it comes to understanding customer reengagement. While prior research has revealed some support for this [19], the failure to support Hypothesis 1 deserves more attention.

This is counterintuitive as one might expect the site's biggest supporters (relative to typical users) to demonstrate a higher level of loyalty after the data breach occurred. This is particularly true given the online context. Wakefield [29] explains that Internet users are more willing to disclose personal information (despite the privacy paradox) when a website creates feelings of positive affect, and that these feelings of positive affect have a greater impact on users' higher levels of concern for privacy. In brick-and-mortar settings, Janakiraman *et al.* [7] found that customers who spent more at retail establishments were more likely to be forgiving after the breach. However, Gao *et al.* [45] found that manipulating the perception of the hotel–customer relationship had a significant effect on how positive customers were about the hotel after it responded to the data breach. They found that if the relationship was communal (extended and relational) rather than exchange (transactional), customer expectations about the hotel's breach response were higher. However, the same customers also were more likely to provide positive

word of mouth if the hotel handled the postbreach recovery well. Furthermore, Chen and Jai [44] found that loyalty-level customers (relational customers) at a hotel were less likely to trust in the hotel and its ability to protect their data post data breach. The literature thus seems context-dependent, even when very similar settings are studied. Potentially, website users who have a previously positive relationship with the site may have higher expectations and more to lose from a breach.

A. Why Customers Return

While favorable attitudes may influence recovery positively (e.g., optimism bias [24]), most customers who were affected appeared to return anyway. This is potentially one of the reasons why research is unable to provide direct recommendations on the handling of data breaches. From the firm's standpoint, if consumers appear to return anyway, there is very little incentive for firms to do anything more than the bare minimum to address the data breach.

A potential explanation is that data breaches are now commonplace enough and customers may prefer to vent rather than retreat. Their coping strategies may invoke inward coping strategies that may cause customers to make changes even if these changes may be superficial and ineffective (e.g., removing a credit card from the account that was already compromised). Another possibility is the level of entrenchment. In our survey responses, several of the site users mentioned that they had already dedicated significant time customizing their account and would be inconvenienced by rebuilding their presence on the site. Their profile or content may be difficult to recreate and therefore result in customers just 'accepting' the reality of the breach and perhaps venting then re-engaging. This may be particularly true for the websites that are specifically designed to overcome the privacy paradox (e.g., social networks). This reaction would be consistent with the anger response to the breach rather than a fear response.

B. Fear Trumps Anger

Our research validates the need to carefully parse negative emotional customer responses. We first confirmed, as others have, that it is not enough to know the extent of negative emotion alone. We address this nuance by tackling fear and anger in conjunction with revisit intentions. There are distinct differences in how anger and fear interact with the customer's decision to leave.

Regardless of our coding method for customer behavior postbreach (manual or programmatic), our hypothesis on anger was not upheld. Even though some negative emotions are correlated (Fear and Anger in Table III, $r = 0.289$, $p < 0.05$), each emotion manifests in different behavioral changes. Research reinforces the notion that speaking out, venting, and conflict arise from anger, whereas fleeing or freezing are knee-jerk, fear-based reactions [59]. As stated in Moons *et al.* [52], the differentiation of fear and anger is such that anger is an appraisal of both certainty (ostensibly with regard to where fault lies) and relative strength in a situation, whereas fear is an emotion that accompanies an appraisal of uncertainty and relative weakness. If we consider that anger is associated with an outward emotional coping strategy (outward EFC), we expect that the user will take action [37]. As discussed, much of the literature assumes that this action would be to leave. However, we find that angry customers do not retreat. Their anger may be expressed in other areas such as prominent complaints leading to reputation damage to the website. We believe this is why so much of the extant research focused on the reputational dimensions of the data breach.

Our most significant research finding is from Hypothesis 3. Notably, we find that fear significantly affects customer behavior outcomes. We noted that data breaches appear to elicit reactions such as "panicked," "frozen," and "afraid." Our article furthers the work of Chatterjee *et al.* [12] and adds a much-needed nuanced interpretation of the impact of fear. Individuals who experience fear after a data breach turn to strategies to deal with their inward emotional feelings (Inward-EFC). This response leads to customers avoiding the situation or seeking alternatives [37].

Several practitioner response frameworks have been put forth in the literature to address security breaches (e.g., [60]). Our findings show that while reputational damages should not be ignored by the firm, they will warrant a different response than those users who react with fear. This further reinforces the need to study differentiated emotions such as fear and anger and resulting response strategies as opposed to a more monolithic approach such as apology and/or compensation (e.g., Sony PlayStation network breach in 2011, Toyota Motor Co. data breach in 2016), or a generic crisis response as advocated by the situational crisis communications framework [60], [61].

C. Managerial Implications

Our research has several managerial implications. For simplicity and coherence, we organize these into two main themes: 1) new insights into defending company reputation and customer engagement, and 2) new IT capability tactics companies facing a data-breach crisis may leverage. First, firms must take action to respond to customer emotions, because those emotions are indicative of the customers' perceptions of risk, control, and agency [52]. For example, Kim *et al.* [17] show that companies may employ strategies ranging from offering compensation to regret and apologies, and that companies should indeed actively monitor social media. However, our findings downplay the benefits of using company goodwill as a reputation defense after a data breach. Managing postbreach monitoring and communications of customer sentiment appears to be of much more importance. Specifically, given evidence from our research we find that less than one-third of customers *fully* reengage with the website postbreach. Therefore, we recommend that firms focus on monitoring customer sentiments expressed post data breach, particularly those indicating fearfulness.

Our major recommendation to managers about customer engagement is the necessity of evolving and expanding previous research to address the most important emotional barriers to customer reengagement. We acknowledge that anger is contagious to a much greater extent than joy or sadness [42] and was the focus for managerial recommendations on restoring reputation postbreach. However, our research suggests that responses

to data breaches should focus on monitoring and addressing fearfulness in their customers. Our results show that fear is the most influential emotion leading to changed behavior and/or lower revisit intentions. We thus suggest that managers take a different approach and instead focus on detecting (via media monitoring and customer service departments) and reassuring frightened customers to alleviate and assuage fear. Alternatively, it is conceivable for the firm to allow customers to vent their negative emotions on platforms of their choice and use it as a data point for capturing concerns (where expressed). Based on those concerns, they can then build messaging to dampen fear.

Previous research has overemphasized the frequency and impact of anger in data breaches, but in fact fear is just as common an emotional result. The Identity Theft Resource Center (in [62]) reported that after their victimization, 69% reported fear and 65% reported rage or anger. Furthermore, Sharp [10] shows that in the period following identity theft, similar proportions of victims reported irritation/anger as compared to anxiety/fear. This lends support to our recommendation of making fearful customers a priority after a data breach. Such fearful customers may be less likely to verbalize their emotion, due to the way that fear leads to feelings of indecisiveness and loss of control [52]. These customers may also feel the effects of fear as shame that their personal details were exposed [62] and thus withdraw from company view.

The ability to address customer fear is our second managerial theme, which we present as a new tactic utilizing IT capabilities. We strongly recommend that managers in marketing and information technology departments coordinate closely and work together to create a strategy focusing on the change in behavior of fearful customers. A crisis response based mainly on marketing will fail to properly reach fearful customers. First, on the marketing front, during a site-wide breach the company's team must be careful to not prioritize the loudest and angriest voices. While these voices may damage company reputation, there will be many quieter (or silent) voices leaving the company after a widespread data breach. Anger is contagious and therefore it risks the possibility of amplification: however, we find that fear is the silent killer. Managers should thus train customer service personnel to recognize that fearful responses come from customers who are most likely to leave. The company must also allocate customer service specialists to first identify fearful customers and then reach out to them directly, as fearful customers may be less willing to engage on social media.

The use of various automated IT solutions such as monitoring customer changes in service usage (web analytics), or even using artificial intelligence approaches may be useful. Chat bots may be suitable in quickly identifying angry versus fearful customers and engaging with them accordingly, allowing angry customers to vent and fearful customers to be reassured. If the breach is personal, the company should realize that not all breached customers will know how to (or want to) reach out to its site. Monitoring sites such as social media sites to identify such personal-level breach events will still be helpful. Moreover, reassuring the customer that the site will help them in rebuilding their profile, and informing them of firm efforts to increase security will be critical as these are concerns raised by the participants in this article.

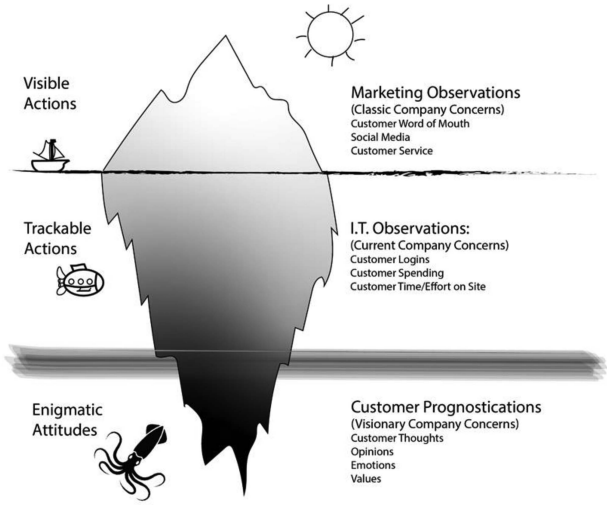


Fig. 2. Company perspective of customer environment.

In order for marketing to be capable of identifying fearful customers with changed habits, they must partner with information technology. This piece has been largely missing in previous research recommendations. The closest to this approach is Gao *et al.* [45], who suggest using social media and online concierges to connect with hotel customers after a breach, and also using an electronic tablet in the hotel room itself. Janakiraman [7] shows customers may cut back on their involvement with the site and may switch to other, undamaged channels. We suggest further, more immersive steps along this line of thought.

Web analytics would allow websites to rapidly detect changed user habits more rapidly than, say, a brick-and-mortar retailer or hotel chain. Our respondents were required to have an account on the affected site. In their response to the data breach participants spoke of taking steps such as removing profile data, logging in less often/never, and other changes that would be visible to the website's information technology managers. These changes in behavior, associated with an increase in fear, are becoming readily detectable using analytics, and may be precursors and act as signals that the customer is leaving the website altogether. An abnormal change in habit by a website user in the wake of a data breach should prompt a contact by the company. This would be a proactive effort as opposed to merely responding on social media. We propose that the contact should not be merely generic (e.g., "It's been a while since you logged in"), but tailored to lowering the customer's fear. Assurance communications could be a powerful reengagement tool when used in this manner. We visualize the change to include customer trackable actions via IT in Fig. 2. This is best portrayed as the visible components of the iceberg (Marketing Observations and IT Observations) versus what lies underneath (Customer Prognostications).

We end our discussion by detailing how our implications about customer fear extend previous research. As companies

TABLE VI
EVOLUTION OF DATA BREACH RESPONSES

	Company Monitoring:	*Company Response, Strategy*	*Company Response, Scope*	*Focus*
Early Company Response Strategies:	None	Denial, Diminishment	Global, One-way Marketing/Public Relations Focus	Repair Reputation
Current Research Recommendations:	News, Social Media	Balance Defensiveness with Accommodation/ Rebuilding	Global, Two-way Marketing and Public Relations Focus	Manage and Monitor Crisis, Lower Intensity of anger
Our Recommendations (to further the evolution of response strategies)	News, Social Media, Individual-level Customer Accounts	Accommodation/ Rebuilding Focus, Individual-level response to finding and reassuring customers	Individualized, High-Tech, Marketing and Information Technology Focus	Manage and Monitor Crisis, Diminish Fear

began engaging in digital transformations, there were fewer data breaches and less social media. In prior studies of data breaches, such as paper [63] by Sinanaj and Zafar, it was documented that data breaches can cause harm to a company's reputation. In these early days, the first emergent responses by firms to data breach events tended to be a denial or diminish strategy [64]–[66] where companies tended to emphasize defending reputation. Thus, many of the recommendations for companies facing data breaches shifted to monitoring social media for intense customer response and reacting to said response in a way that protects the company's reputation. These recommendations also tended to highlight whether the company has a relatively full "reservoir of goodwill" [67]. More current research, e.g., [41] implies that managers should minimize feelings of anger in customers after data breaches. Syed [41] found that negative emotions such as anger and disgust are likely to increase reputation threats against a firm that has suffered a data breach. We move these managerial implications forward by using advances in technology to target fearful customers post data breach. Table VI provides a summary of the evolution of firm responses to data breaches, and situates our findings as a way to continue this evolution in a more detailed and responsive manner.

VII. CONCLUSION

In this article, we show that customers have a distinct emotional response to a data breach consisting of fear and anger. We find that based on the experienced emotion, customers take different actions, and that negative emotions need to be dissected and studied separately. Angry customers may vent and produce reputational damage but tend to continue their usage. On the other hand, fearful customers make furtive changes, or leave the website all together. This article contributes to the literature by deepening our understanding of consumer's emotional reaction and subsequent action in light of a data breach. These findings have important managerial implications, demonstrating that a monolithic response to a data breach may be improved by using technology to segment angry versus fearful customers and devising targeted responses based on customer's emotional response.

Our article is not without limitations. First, customers may have widely different valuations of the information stolen or destroyed in a data breach. For example, a survey of customers showed that 54% were most afraid of their social security numbers being stolen, 18% were most afraid of banking information, while only 9% were most afraid of their credit card being stolen [68]. It may be useful to separate the theft of sentimental content (e.g., photos of family and friends) compared to, say, artistic or financial items.

Another limitation is the technological knowledge of users. While we did measure educational background, that is only a proxy for how aware users are of the effects of a data breach. We note that the effect of fear on customer decision-making could be dependent on factors such as how much they know about the details and consequences of the breach, their experience with technology, and other key factors. We acknowledge that these factors need to be studied as they were not considered in this article. Future research might include measures such as internet privacy concerns, personal characteristics such as self-efficacy, experience with the Internet, prior experience with data breaches, and level of engagement with site.

Future research could be more specific in examining how the reported details of the data breach (e.g., description of the data breached) change emotional responses of the users. For example, customers may base their response on what they are told about the site's culpability in the breach. In addition, future research could include more precise measurements of a user's attachment to the site (e.g., time spent on site per week) and whether the user is aware of existing substitutes or alternatives to the site in question. Finally, the research could potentially be improved by asking customers to more specifically rate their likelihood of making changes from a list of alternatives (remove payment information, delete logins, use anonymously, consider competitors, leave for a time, reduce engagement, seek immediate alternatives, etc.).

REFERENCES

[1] WOF, "US adults added 1 hour of digital time in 2020," *Insider Intelligence*. Accessed: Jun. 25, 2021. [Online]. Available: https://www.emarketer.com/content/us-adults-added-1-hour-of-digital-time-2020

[2] Coronavirus Internet Use, New York Times, Apr. 7, 2020. [Online]. Available: https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html

[3] Tankovska, "Global time spent with online video 2020," Statista, 2020. Accessed: Jul. 28, 2021. [Online]. Available: https://www.statista.com/statistics/611707/online-video-time-spent/

[4] C. Shearman, "March retail sales see strong rebound amid increased vaccination and government stimulus," NRF, 2020. Accessed: Jun. 20, 2021. [Online]. Available: https://nrf.com/media-center/press-releases/march-retail-sales-see-strong-rebound-amid-increased-vaccination-and

[5] Identity Theft Resource Center, "The ITRC 2020 data breach report reveals good and bad news for businesses and consumers," Jan. 28, 2021. Accessed: Jun. 2, 2021. [Online]. Available: https://www.idtheftcenter.org/the-itrc-2020-data-breach-report-reveals-good-and-bad-news-for-businesses-and-consumers/

[6] CNBC, "T-Mobile says data on 40 million people stolen by hackers," 2021, Accessed: Aug. 25, 2021. [Online]. Available: https://www.cnbc.com/2021/08/18/t-mobile-hackers-stole-about-7point8-million-customers-personal-data.html

[7] R. Janakiraman, J. H. Lim, and R. Rishika, "The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer," *J. Marketing*, vol. 82, no. 2, pp. 85–105, 2018.

[8] I. Confente, G. G. Siciliano, B. Gaudenzi, and M. Eickhoff, "Effects of data breaches from user-generated content: A corporate reputation analysis," *Eur. Manage. J.*, vol. 37, no. 4, pp. 492–504, 2019.

[9] R. Chakraborty, J. Lee, S. Bagchi-Sen, S. Upadhyaya, and H. R. Rao, "Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults," *Decis. Support Syst.*, vol. 83, pp. 47–56, 2016.

[10] T. Sharp, A. Shreve-Neiger, W. Fremouw, J. Kane, and S. Hutton, "Exploring the psychological and somatic impact of identity theft," *J. Forensic Sci.*, vol. 49, no. 1, pp. 1–6, 2004.

[11] E. Bachura, R. Valecha, R. Chen, and H. R. Rao, "Data breaches and the individual: An exploratory study of the OPM hack," in *Proc. Int. Conf. Inf. Syst.*, Dec. 2017, pp. 1–9. [Online]. Available: https://aisel.aisnet.org/icis2017/HumanBehavior/Presentations/26

[12] S. Chatterjee, X. Gao, S. Sarkar, and C. Uzmanoglu, "Reacting to the scope of a data breach: The differential role of fear and anger," *J. Bus. Res.*, vol. 101, pp. 183–193, 2019.

[13] A. Malhotra and C. K. Malhotra, "Evaluating customer information breaches as service failures: An event study approach," *J. Service Res.*, vol. 14, no. 1, pp. 44–59, 2011.

[14] J. D. Elhai and B. J. Hall, "Anxiety about internet hacking: Results from a community sample," *Comput. Hum. Behav.*, vol. 54, pp. 180–185, 2016.

[15] A. J. Burns, C. Posey, T. L. Roberts, and P. B. Lowry, "Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals," *Comput. Hum. Behav.*, vol. 68, pp. 190–209, 2017.

[16] A. Kankanhalli, H.-H. Teo, B. C. Tan, and K.-K. Wei, "An integrative study of information systems security effectiveness," *Int. J. Inf. Manage.*, vol. 23, no. 2, pp. 139–154, 2003.

[17] B. Kim, K. Johnson, and S.-Y. Park, "Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity," *Cogent Bus. Manage.*, vol. 4, no. 1, pp. 1–15, 2017, doi: 10.1080/23311975.2017.1354525.

[18] K. Berezina, C. Cobanoglu, B. L. Miller, and F. A. Kwansa, "The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth," *Int. J. Contemporary Hospitality Manage.*, vol. 24, no. 7, pp. 991–1010, 2012.

[19] K. Gwebu, J. Wang, and L. Wang, "The role of corporate reputation and crisis response strategies in data breach management," *J. Manage. Inf. Syst.*, vol. 35, no. 2, pp. 683–714, 2018.

[20] M. Kesgin and R. S. Murthy, "Consumer engagement: The role of social currency in online reviews," *Service Industries J.*, vol. 39, no. 7/8, pp. 609–636, 2019.

[21] N. K. Lankton, D. H. McKnight, and J. F. Tripp, "Understanding the antecedents and outcomes of Facebook privacy behaviors: An integrated model," *IEEE Trans. Eng. Manage.*, vol. 67, no. 3, pp. 697–711, Aug. 2020.

[22] P. Van Schaik, D. Jeske, J. Onibokun, L. Coventry, J. Jansen, and P. Kusev, "Risk perceptions of cyber-security and precautionary behaviour," *Comput. Hum. Behav.*, vol. 75, pp. 547–559, 2017.

[23] M. Workman, W. H. Bommer, and D. Straub, "The amplification effects of procedural justice on a threat control model of information systems security behaviours," *Behav. Inf. Technol.*, vol. 28, no. 6, pp. 563–575, 2009.

[24] Y. Zou and F. Schaub, "Beyond mandatory: Making data breach notifications useful for consumers," *IEEE Secur. Privacy*, vol. 17, no. 2, pp. 67–72, Mar. 2019.

[25] C. P. Hoffmann, C. Lutz, and G. Ranzini, "Privacy cynicism: A new approach to the privacy paradox," *Cyberpsychol. J. Psychosocial Res. Cyberspace*, vol. 10, no. 4, pp. 1–18, 2016.

[26] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Comput. Secur.*, vol. 64, pp. 122–134, 2017.

[27] D. L. Mothersbaugh, W. K. Foxx, S. E. Beatty, and S. Wang, "Disclosure antecedents in an online service context: The role of sensitivity of information," *J. Serv. Res.*, vol. 15, no. 1, pp. 76–98, 2012.

[28] L. Baruh, E. Secinti, and Z. Cemalcilar, "Online privacy concerns and privacy management: A meta-analytical review," *J. Commun.*, vol. 67, no. 1, pp. 26–53, 2017.

[29] R. Wakefield, "The influence of user affect in online information disclosure," *J. Strategic Inf. Syst.*, vol. 22, no. 2, pp. 157–174, 2013.

[30] S. Mamonov and M. Koufaris, "The impact of perceived privacy breach on smartphone user attitudes and intention to terminate the relationship with the mobile carrier," *Commun. Assoc. Inf. Syst.*, vol. 34, Mar. 2014, Art. no. 1, doi: 10.17705/1CAIS.03460.

[31] J. Boehmer, R. LaRose, N. Rifon, S. Alhabash, and S. Cotten, "Determinants of online safety behaviour: Towards an intervention strategy for college students," *Behav. Inf. Technol.*, vol. 34, no. 10, pp. 1022–1035, 2015.

[32] R. Crossler and F. Bélanger, "An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument," *ACM SIGMIS Database DATABASE Adv. Inf. Syst.*, vol. 45, no. 4, pp. 51–71, 2014.

[33] H. Liang and Y. Xue, "Understanding security behaviors in personal computer usage: A threat avoidance perspective," *J. Assoc. Inf. Syst.*, vol. 11, Jul. 2010, Art. no. 7, doi: 10.17705/1jais.00232.

[34] H. S. Tsai, M. Jiang, S. Alhabash, R. LaRose, N. J. Rifon, and S. R. Cotten, "Understanding online safety behaviors: A protection motivation theory perspective," *Comput. Secur.*, vol. 59, pp. 138–150, Jun. 2016, doi: 10.1016/j.cose.2016.02.009.

[35] H. Choi, J. Park, and Y. Jung, "The role of privacy fatigue in online privacy behavior," *Comput. Hum. Behav.*, vol. 81, pp. 42–51, 2018.

[36] M. Lee and J. Lee, "The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet," *Inf. Syst. Front.*, vol. 14, no. 2, pp. 375–393, 2012.

[37] H. Liang, Y. Xue, A. Pinsonneault, and Y. Wu, "What users do besides problem-focused coping when facing it security threats: An emotion-focused coping perspective," *MIS Quart.*, vol. 43, no. 2, pp. 373–394, 2019.

[38] H. Liang and Y. Xue, "Avoidance of information technology threats: A theoretical perspective," *MIS Quart.*, vol. 33, no. 1, pp. 71–90, 2009, doi: 10.2307/20650279.

[39] R. P. Bagozzi, "The self-regulation of attitudes, intentions, and behavior," *Soc. Psychol. Quart.*, vol. 55, no. 2, pp. 178–204, 1992, doi: 10.2307/2786945.

[40] R. S. Lazarus, *Emotion and Adoption*. Oxford, U.K.: Oxford Univ. Press, 1991.

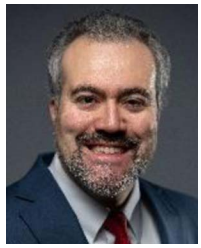
[41] R. Syed, "Enterprise reputation threats on social media: A case of data breach framing," *J. Strategic Inf. Syst.*, vol. 28, no. 3, pp. 257–274, Sep. 2019, doi: 10.1016/j.jsis.2018.12.001.

[42] R. Fan, J. Zhao, Y. Chen, and K. Xu, "Anger is more influential than joy: Sentiment correlation in weibo," *PLoS ONE*, vol. 9, no. 10, Oct. 2014, Art. no. 110184, doi: 10.1371/journal.pone.0110184.

[43] Z. Aivazpour, R. Valecha, and R. Chakraborty, "The impact of data breach severity on post-breach online shopping intention," in *Proc. Int. Conf. Inf. Syst.*, Dec. 2018. [Online]. Available: https://aisel.aisnet.org/icis2018/security/Presentations/13/

[44] H. S. Chen and T.-M. C. Jai, "Cyber alarm: Determining the impacts of hotel's data breach messages," *Int. J. Hospitality Manage.*, vol. 82, pp. 326–334, 2019.

[45] Y. L. Gao, L. Zhang, and W. Wei, "The effect of perceived error stability, brand perception, and relationship norms on consumer reaction to data breaches," *Int. J. Hospitality Manage.*, vol. 94, 2021, Art. no. 102802.
[46] M. C. Arcuri, L. Gai, F. Ielasi, and E. Ventisette, "Cyber attacks on hospitality sector: Stock market reaction," *J. Hospitality Tourism Technol.*, vol. 11, no. 2, pp. 277–290, 2020.
[47] K. Gwebu and C. W. Barrows, "Data breaches in hospitality: Is the industry different?," *J. Hospitality Tourism Technol.*, vol. 11, no. 3, pp. 511–527, 2020.
[48] M. Zeelenberg, R. M. Nelissen, S. M. Breugelmans, and R. Pieters, "On emotion specificity in decision making: Why feeling is for doing," *Judgment Decis. Mak.*, vol. 3, no. 1, pp. 18–27, 2008.
[49] S. Folkman, R. S. Lazarus, C. Dunkel-Schetter, A. DeLongis, and R. J. Gruen, "Dynamics of a stressful encounter: Cognitive appraisal, coping, and encounter outcomes," *J. Pers. Social Psychol.*, vol. 50, no. 5, pp. 992–1003, 1986.
[50] Z. C. Li and D. Stacks, "When the relationships fail: A microperspective on consumer responses to service failure," *J. Public Relations Res.*, vol. 29, no. 4, pp. 158–175, 2017.
[51] K. D. Martin, A. Borah, and R. W. Palmatier, "Data privacy: Effects on customer and firm performance," *J. Marketing*, vol. 81, no. 1, pp. 36–58, 2017.
[52] W. G. Moons, N. I. Eisenberger, and S. E. Taylor, "Anger and fear responses to stress have different biological profiles," *Brain, Behav., Immun.*, vol. 24, no. 2, pp. 215–219, 2010.
[53] I. J. Roseman, "Cognitive determinants of emotion: A structural theory," *Rev. Pers. Social Psychol.*, vol. 5, pp. 11–36, 1984.
[54] R. Layton and P. A. Watters, "A methodology for estimating the tangible cost of data breaches," *J. Inf. Secur. Appl.*, vol. 19, no. 6, pp. 321–330, 2014.
[55] J. N. Angelis and J. C. Miller, "An empirical investigation of the effects of individuality on responses to data theft crimes," *IEEE Trans. Eng. Manage.*, vol. 68, no. 6, pp. 1663–1676, Dec. 2021, doi: 10.1109/TEM.2020.2974742.
[56] N. Manworren, J. Letwat, and O. Daily, "Why you should care about the target data breach," *Bus. Horiz.*, vol. 59, no. 3, pp. 257–266, May 2016, doi: 10.1016/j.bushor.2016.01.002.
[57] F. Khan, J. H. Kim, L. Mathiassen, and R. Moore, "Data breach management: An integrated risk model," *Inf. Manage.*, vol. 58, no. 1, 2021, Art. no. 103392.
[58] R. Sen and S. Borle, "Estimating the contextual risk of data breach: An empirical approach," *J. Manage. Inf. Syst.*, vol. 32, no. 2, pp. 314–341, 2015.
[59] J. S. Lerner and D. Keltner, "Beyond valence: Toward a model of emotion-specific influences on judgement and choice," *Cogn. Emotion*, vol. 14, no. 4, pp. 473–493, 2000.
[60] C. Onwubiko and K. Ouazzane, "SOTER: A playbook for cybersecurity incident management," *IEEE Trans. Eng. Manage.*, to be published, doi: 10.1109/TEM.2020.2979832.
[61] W. T. Coombs, "Protecting organization reputations during a crisis: The development and application of situational crisis communication theory," *Corporate Reputation Rev.*, vol. 10, no. 3, pp. 163–176, 2007.
[62] K. Golladay and K. Holtfreter, "The consequences of identity theft victimization: An examination of emotional and physical health outcomes," *Victims Offenders*, vol. 12, no. 5, pp. 741–760, 2017.
[63] G. Sinanaj and H. Zafar, "Who wins in a data breach? A comparative study on the intangible costs of data breach incidents," in *Proc. Pac. Asia Conf. Inf. Syst.*, 2016, pp. 1–14.
[64] S. Kim and B. F. Liu, "Are all crises opportunities? A comparison of how corporate and government organizations responded to the 2009 flu pandemic," *J. Public Relations Res.*, vol. 24, no. 1, pp. 69–85, 2012.
[65] H. F. Sisco, E. L. Collins, and L. M. Zoch, "Through the looking glass: A decade of red cross crisis response and situational crisis communication theory," *Public Relations Rev.*, vol. 36, no. 1, pp. 21–27, 2010.
[66] H. J. Kim and G. T. Cameron, "Emotions matter in crisis: The role of anger and sadness in the publics' response to crisis news framing and corporate crisis response," *Commun. Res.*, vol. 38, no. 6, pp. 826–855, 2011.
[67] G. H. Jones, B. H. Jones, and P. Little, "Reputation as reservoir: Buffering against loss in times of economic crisis," *Corporate Reputation Rev.*, vol. 3, no. 1, pp. 21–29, 2000.
[68] N. J. Manwah, "Americans fear for their data more than their wallet, radware survey finds," 2018. Accessed: Jun. 20, 2021. [Online]. Available: https://radware.com/newsevents/pressreleases/2018/americans-fear-for-their-data



John N. Angelis received the B.E degree in industrial and systems engineering from Youngstown State University, Youngstown, OH, USA, in 2002, and the Ph.D. degree in operations research from Case Western University, Cleveland, OH, in 2009.

His previous work experience was with General Electric Lighting and the United States government. He is currently an Assistant Professor of Operations with the School of Business, University of Lynchburg, Lynchburg, VA, USA. His research interests include mathematically modeling entrepreneurial decision-making, analyzing the effects of innovation and technology on customer behavior and firm performance, and sports analytics.

Dr. Angelis was the recipient of the Distinguished Service Award from the Technology, Innovation, Management and Entrepreneurship Society of INFORMS, the Gold Star Teaching Award from the University of Wisconsin-Milwaukee, and the Ohio Board of Regents Fellowship. He is a member of AOM and INFORMS, and has served on the IEEE Transactions on Engineering Management Editorial Board since 2014.

Rajendran S. Murthy received the Ph.D. degree in marketing from Southern Illinois University, Carbondale, IL, USA, in 2009.

He is the J. Warren McClure Research Professor in marketing with the Saunders College of Business, Rochester Institute of Technology, Rochester, NY, USA. His research is tied strongly to his experience and his teaching interests in the domain of quantitative analytics, research methods and branding. His research has been featured in the Harvard Business Review (2 cases) and MIT's Sloan Management Review as well as published in top academic journals such as the *Journal of Management*, *Journal of Marketing Management*, IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, and *Business Horizons*. His primary research interests include the design and execution of data-driven consumer engagement strategies.

Tanya Beaulieu received the Ph.D. degree in management information systems from Washington State University, Pullman, WA, USA, in 2015.

She is an Associate Professor with the University of Maine, Orono, ME, USA. She has published in outlets such as *MIS Quarterly, Communications of the Association for Information Systems,* and the *Journal of Computer Information Systems*, as well as proceedings such as the *International Conference of Information Systems* (ICIS). She previously served as the Managing Editor of the *Journal of the Association for Information Systems* (JAIS), and is currently serving as an Associate Editor for *Communications of the Association for Information Systems.* She owned a software development and consulting firm specializing in custom software development for large enterprise systems. Her research interests include communication in online communities, crowdfunding, and entrepreneur's use of technology.

Joseph C. Miller received the Ph.D. degree in marketing from Eli Broad College of Business, Michigan State University, East Lansing, MI, USA, in 2010.

He is a Professor of Marketing and Sales with the Patricia VanBruwaene College of Business, St. Ambrose University, Davenport, IA, USA. He worked as a Marketing/IT consultant in several industries in Southeastern Michigan, including automotive, banking, public sector software, and insurance, and economic development. His work has been published in outlets including *Academy of Management Journal*, *Harvard Business Review*, *Journal of World Business*, and *International Journal of Tourism Sciences*, and published proceedings in leading conferences representing the business disciplines of marketing, global business, and operations. His research interests include service strategy, service failure, and consumer response strategy and failure in situational contexts.

Dr. Miller is a member of the American Marketing Association and the Academy of Marketing Science.