Identity Theft Victims: Critical Influencers for Customer Loyalty Restoration

Thomas M. Brill
University of Dallas
tbrill@udallas.edu

Abstract

In recent years, the number of consumers experiencing identity theft has grown significantly as a result of the explosive growth in personal information stolen through corporate cyber-breaches. While the resultant incidences of credit card fraud linked to this stolen information continue, the scope of identity theft has expanded to involve larger and more complex fraud implications for these consumers which can negatively impact efforts by companies to cultivate and retain loyal customers. Research has identified many of the traditional decision-making factors influencing consumer brand and loyalty selections with the cyber-breached company, but this research omits any direct linkage of the wider identity theft impacts upon these decision-making factors for impacted victims. This mixed method research paper seeks to understand the customer decision-making attitudes and behavioral processes associated with the research question: "*What factors positively influence the restoration of customer loyalty after identity theft?"* Customer loyalty is import to the financial success of the company (Li & Green, 2011). This research is important because it will provide insights into the research gaps associated with the compromised level of trust and commitment in companies by identity theft victims as well as the increasing possibility of spillover impacts being attributed to other companies.

Introduction

Customer loyalty is important to the financial success of a company (Li & Green, 2011). The relational bond between the customer and the company is premised upon the foundational components of trust, commitment (Evanschitzky et al., 2012; Haelsig, Swoboda, Morschett, & Schramm-Klein, 2007) and satisfaction (Evanschitzky et al., 2012). This paper will define identity theft and its expanding negative impact on individual victims; examine situations whereby individuals become aware that they have become victims of identity theft; review the concept of spillover blame attribution associated with cyber-breaches; and associate these implications of identity theft to certain principles of trust and customer loyalty.

Literature Review

Identity Theft

"[Cyber-] breaches involve unauthorized access to personal information, resulting from a variety of security incidents including hackers breaking into systems or networks, third parties accessing personal information on lost laptops or other mobile devices, or organizations failing to dispose of personal information securely" (Culnan & Williams, 2009, p. 675). Outcomes of such unauthorized access can include breach of confidentiality and trust, or financial harm to the individual resulting from identity theft or fraud (Culnan & Williams, 2009; SafeNet, 2014).

The fastest growing crime in America is identity theft, and it impacts millions of people each year (Eisenstein, 2008; Pagliery, 2015). The scope of identity theft is not limited to the United States as it is a growing problem throughout the world as well (Archer, Sproule, Yuan, Guo, & Xiang, 2012). Identity theft is defined as the knowing transfer, possession, or usage of any name or number that identifies another person, with the intent of committing or aiding or abetting a crime accounts (Benton, Blair, Crowe & Schuh, 2007).

The scope of crimes associated with identity theft include credit card fraud, credit application fraud, social security claim fraud (Chicago Tribune, 2015), income tax return fraud (Cohen, 2015), pension withdrawal fraud, medical claim fraud (Shinal, 2015), and blackmail (Benton et al., 2007; Evanschitzky et al., 2012; Haelsig et al., 2007). Still, these monetary costs are generally only part of the total impact incurred by the victim (Eisenstein, 2008). For many consumers, the emotional impact of breach of confidentiality and trust (Ping, Ishaq, & Li, 2015) is the more damaging and longer lasting outcome of identity theft (Burns & Stanley, 2002).

A major obstacle limiting identity theft research is the variety of ways in which terms are used (Smith & Hart, 2011; Solove, 2006). The lack of a consistent taxonomy allows many different crimes to include the use or abuse of another's identity or identity related factors (Copes, Kerley, Huff, & Kane, 2010; Newman & McNally, 2005). Despite this limitation, there is alignment that identity theft negatively impacts the levels of user trust (Kahn & Liñares-Zegarra, 2012). This negative user trust is reflected in two ways. First, it creates fears of victimization (Copes et al., 2010). Second, it reduces trust in the safety and reliability of commercial interactions with companies (Copes et al., 2010). From a fundamental economic perspective of identity theft, these two negative trust impacts affect consumers' expectations of the cost and benefits of engaging in a trusting and loyal relationship with a provider (Kahn & Liñares-Zegarra, 2012) and are components to be explored in this research.

> *P1. Company commitment, trust and satisfaction has a positive relationship with the customer's perception of the brand.*

Delayed Recognition of Identity Theft

As a result of the cyber-breach notification laws, affected individuals are required to be notified of the cyber-breach by the impacted firm (Culnan & Williams, 2009; Ponemon Institute, 2014). While the intent of the notifications is to increase awareness and transparency, there is little consistency and a high amount of complexity in most notices (Romanosky, Telang, & Acquisti, 2011). As such, only portions of the impacted population are being made aware of the risks associated with identity theft (Romanosky et al., 2011; Ponemon, 2014). Some of the population understand these notifications and have realized that the incidents compromised their personal privacy (Ponemon, 2014). Many now have a heightened fear that identity theft is likely or have been forced to deal with the realities of actual identity theft (Ponemon, 2014). As a result, many of the impacted individuals now perceive that the firm allowed a violation of trust and commitment to occur (Malhotra & Malhotra, 2010). This violation is subsequently reflected in the customer's negative trust and commitment evaluations of the firm which impacts the likelihood of a customer continuing to be loyal (Evanschitzky et al., 2012; Haelsig et al., 2007).

For the remaining group of affected individuals, there generally is very little awareness created at the time of the notice. Some individuals ignore the notice in its entirety (Peltier, Milne, & Phelps, 2009; Phelps & Milne, 2009); Romanosky et al., 2011; Ponemon, 2014). Others fail to react to the notice because they have received too many notices and are becoming either desensitized or confused about the risk (Romanosky et al., 2011; Ponemon, 2014). At some point, these individuals will likely recognize that they too are identity theft victims (Peltier et al., 2009; Phelps & Milne, 2009; Romanosky et al., 2011; Ponemon, 2014).

Research currently has ignored examining how long this delayed awareness may last and what these individuals will think and do once they become aware of the identity theft. Given the increasing probability that individuals will be victims of more than one cyber-breach (Acquisti, Taylor, & Wagman, 2014), there is a research gap in assessing if the individual will be able to attribute the trust and commitment violation to the proper firm. Once an individual perceives that a firm has violated a trust or commitment, the possibility of a trust or loyalty relationship fracture is introduced in the decision-making process of the individual (Steinhoff & Palmatier, 2014; Xia & Kukar-Kinney, 2014). This research examines critical influencers for developing a strong and loyal relationship in a post-breach environment.

> *P2. The positive relationship between the company's promise and the perception of the brand is partially mediated by the individual's awareness of being an identity theft victim.*

Corporate Crises Spillover Effects

Product harm crises are events when the products or services provided are found to be substandard, malfunctioning or risky (Dawar & Pillutla, 2000; Siomkos & Malliaris, 2011). The 'spillover component effect' reflects customer perception that the product harm crisis is not unique to a particular company's product or service but is applicable to similar products within the industry (Ping et al., 2015).

Cyber-breach corporate crises (a form of product harm crisis) are becoming more frequent (Acquisti et al., 2014). Even though the affected firm must deal with the direct impacts of the crisis, research identifies that some crises can have spillover impacts on similar brands in the industry (Roehm & Tybout, 2006; Lei, Dawar, & Lemmink, 2008; Vassilikopoulou, Siomkos, Chatzipanagiotou, & Pantouvakis, 2009; Ping et al., 2015). The crises results can have negative impacts for multiple parties, such as injuries to consumers (Papadakis, 2006; Goss, Silvera, DLaufer, Gillespie, & Arsena, 2011), a destroyed public image and reputation (Mowen, 1980; Siomkos, 1999), and a lack of consumer confidence in the affected company (Dawar & Pillutla, 2000; Dawar & Lei, 2009).

Once loyal customers now are vulnerable due to compromised levels of trust in the firm (Siomkos, 1999; Ma, Zhang, Wang, & Li, 2014)). This trust reduction is reflected in negative purchase intentions (Pruitt & Peterson, 1986; Siomkos & Kurzbard, 1994; Tsang, 2000; Laufer & Gillespie, 2004) and a shift to competitor brands (Cleeren, Dekimpe, & Helsen, 2006). As a result, the company is likely to record lower sales which then can introduce negative pressure on stock prices (Pruitt & Peterson, 1986; Siomkos & Kurzbard, 1994). These effects are directly related to the research question for this study.

Firms susceptible to potential spillover impacts must be mindful of the crisis' impact on consumer attribution of blame (Ping et al., 2015). The blame attribution may or may not be justified to the firm, but it does reflect consumer perception (Siomkos & Malliaris., 2011). The attribution of blame generally is reflected in a reduction in trust and a reduction in commitment and loyalty to the brand (Dahlen & Lange, 2006; Ping et al., 2015). At this point, the research on the spillover effects of product harm crises is still in its infancy (Klein & Dawar, 2004; Ping et al., 2015). This research lacks dimensional implications associated with the delayed consumer awareness of identity theft and the spillover of wide-broadcast blame attribution from non-industry firms. The negative impact of these two items on trust is directly related to the research question.

Litigation associated with blame attribution is also experiencing change implications for cyber-breach linked companies. Past court rulings have required confirmation of actual unreimbursed identity theft, but that approach is now being altered to allow for the risk of identity theft as being sufficient grounds for litigation (Nash, 2015). Not only does this expose companies to the risk of costly legal challenges and punitive awards but chief information officers and other senior executives are also likely to face legal battles stemming from cyber-breach failures (Nash, 2015). While an effective loyalty program is not expected to stop this litigation, it might serve as a possible deterrent to large liability litigation for damages from a cyber-breach. As such, this research will provide insights which can contribute to an effective loyalty program in a post-breach environment.

> *P3. The partially mediating relationship of identity theft victim awareness to the perception of the brand is partially mediated by the attribution of blame for the identity theft.*

> *P4. The relationship between the identity theft victim awareness and the attribution of blame is positively moderated by the perceived magnitude of the impact of the identity theft.*

Customer Loyalty

In the consumer marketing community, customer loyalty has long been regarded as an important goal (Reichheld & Schefter, 2000). Numerous studies have identified that delighting customers and delivering superior value through excellent services and quality products are two effective contributors towards creating customer loyalty (Lee, Lee, & Feick, 2001; Yang & Peterson, 2004; Li & Green, 2011). Customer loyalty is important because it provides a consistent pipeline for revenues while lowering customer acquisition costs and yielding increased profits (Li & Green, 2011).

Many companies are introducing incentive loyalty programs reflecting certain basic components of the Social Exchange Theory (Chen, Chen, & Farn, 2010) and the Equity Theory (Evanschitzky et al., 2012). The Social Exchange Theory predicts that people attempt to reciprocate to those who benefit them (Bateman & Organ, 1983; Chen et al., 2010; Wang, Hsu, and Chih, 2014). The Equity Theory focuses upon a person's perception of fairness with respect to a relationship (Huseman, Hatfield, & Miles, 1987). These definitions form the premise of the loyalty program that customers who perceive value in the relationship with the company will demonstrate higher degrees of loyalty to that company as long as the customer perceives that the company is trusting, committed and fair to the customer (Li & Green, 2011; Steinhoff & Palmatier, 2014; Xia & Kukar-Kinney, 2014).

The program also leverages a customer's investment of time (e.g., duration of membership), knowledge (e.g., referral and endorsement recommendations) and economics (e.g., amount of money spent) to create a perception that the customer has achieved an exceptional status (Cho & Song, 2012). The strength of the customer's perception of this earned status creates a psychological and economic barrier to switch to another provider (Evanschitzky et al., 2012; Xia & Kukar-Kinney, 2014; Davcik, Vinhas, & Hair, 2015).

The service failure and dissatisfaction experienced with a cyber-breach are major negative events influencing loyalty (Cho & Song, 2012). If customers do not trust that their personal information is secured and executed within their perceived authorized scope, the customers will not use a particular provider (Urban, Sultan, & Qualls, 2000). Since perceptions of trust is a key decision-making element in determining loyalty, care must be taken to preserve this trusting relationship. Trusting relationships which have experienced a fracturing event(s) are notoriously hard to repair and re-establish (Rempel, Holmes & Zanna, 1985; King-Casas et al., 2008). However, the greater the relationship experience (including incentives and benefits) before a trust breach occurs, the higher the likelihood that the company will be able to re-establish some level of a trusting relationship following a cyber-breach (Schilke, Reimann, & Cook, 2013; Datacandy.com, 2014). In this situation, the relationship is likely to continue as long as the negative relational elements are perceived to be a price worth paying in order to retain the positive relational element (Petriglieri, 2015). If such a provider relationship doesn't exist, then identity theft victims favor trusted brands (Petriglieri, 2015).

Scholars have only recently begun to focus on the recovery of trust and loyalty following an identity theft associated with a cyber breach (Schilke et al., 2013). This prior lack of focus has exposed a gap in the breadth and depth of research literature in this area. Extant research also fails to account for the interactive effects of multiple psychological components (e.g., perceptions of fairness) within an individual's loyalty decision-making process (Steinhoff & Palmatier, 2014; Xia & Kukar-Kinney, 2014). This research will contribute insights toward the establishment of a stronger loyal relationship with a customer.

The Impact of Trust on Loyalty

The importance of protecting the privacy of an individual's personal information is a multidimensional and deeply personal concept that varies with a person's life experiences (Xu, Dinev, Smith, & Hart, 2008). These life experiences also include an overlap of new technology considerations (Brill, 2014). The combination of individual life experiences and personal beliefs has a significant impact on how individuals determine the appropriateness of what, why, how, and to whom they provide their personal information (Martin & Parmar, 2012). Inherent in this discourse is the concept of a social contract between the provider and the individual.

Under the social contract mindset, customers provide certain personal information to a provider with the expectation that the provider will protect the personal information from unauthorized access and disclosure by others (Brill, 2014). Much of a consumer's willingness to provide personal information depends on a consumer's evaluation of the perceived risks and benefits of disclosure (D'Souza & Phelps 2009; Milne, Rohm, & Boza 1999; Milne & Rohm 2000; Norberg, Horne, & Home, 2007; Milne, Gabisch, Markos, & Phelps, 2012). Given the growth in the volume of cyber-breaches (Acquisti et al., 2014), this social contract is being compromised (Brill, 2014). The negative impact of the breach of trust serves to be an obstacle for retaining customer loyalty (Evanschitzky et al., 2012, Haelsig et al., 2007). Once a breach of trust occurs, trust is notoriously hard to reestablish (Schilke et al., 2013).

The service recovery theory provides some insights on the impacts of the breach of trust upon customer loyalty. When instances of service failures occur, the service recovery theory states that an effective recovery approach can enhance relationship quality and enhance customer retention (Fornell & Wernerfelt, 1987). The relationship quality consists of the customer evaluation of trust, commitment and satisfaction (Oly Ndubisi, 2006). When based upon the principles of the service recovery theory, properly designed and executed service recovery programs, including atonement incentives or benefits (Boshoff, 2005), can help to retain customers (Wang et al., 2014). At present, there is little extant research examining the linkages of delayed recognition of identity theft trust and commitment issues to the service recovery theory and the victim's perception of value and benefit associated with identity wellness tools. This research will contribute insights enabling future research for this important topic.

> *P5. The positive relationship between the perception of the brand and the customer's loyalty to the brand is positively moderated by victim's perception of value and benefit associated with identity wellness tools.*

Summary

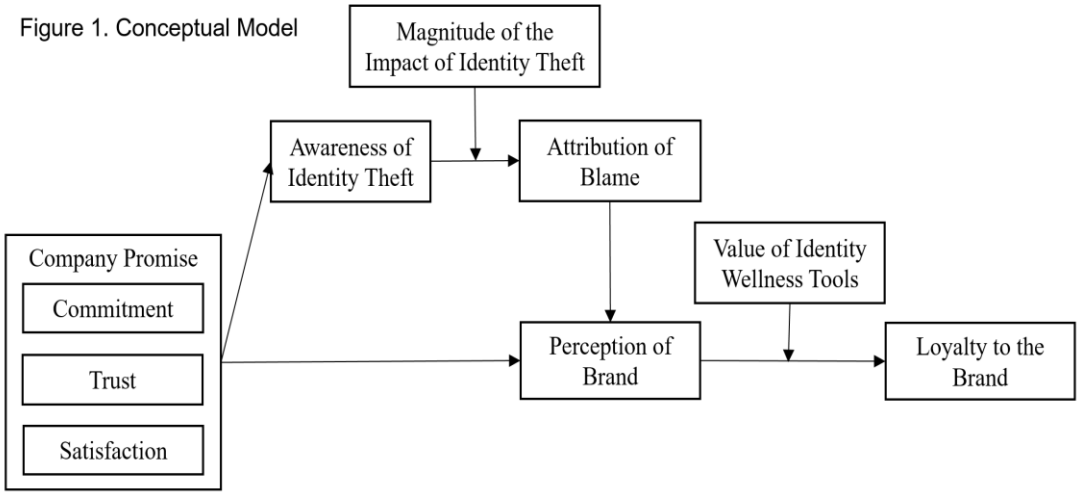
Customer loyalty is import to the financial success of the company (Li & Green, 2011). The affective relational bond between the customer and the company is premised upon the foundational components of trust, commitment (Evanschitzky et al., 2012; Haelsig et al., 2007) and satisfaction (Evanschitzky et al., 2012). These foundational components can be compromised when customers become victims of identity theft as a result of a cyber-breach (Culnan & Williams, 2009). Customer loyalty programs assist in deepening the affective relational bond with the company which proves beneficial in regaining customer trust after a service recovery incident (Wang et al., 2014). However, research gaps exist as scholars have only recently begun to focus on the recovery of trust following a breach (Schilke et al., 2013) as well as the interactive effects of multiple psychological components (e.g., perceptions of fairness) within an individual's loyalty decision-making process (Steinhoff & Palmatier, 2014; Xia & Kukar-Kinney, 2014).

Even though cyber-breach victims are notified of the incident, some individuals ignore the notice in its entirety (Peltier et al., 2009; Phelps & Milne, 2009); Romanosky et al., 2011; Ponemon, 2014). Others fail to react to the notice because they have received too many notices and are becoming either desensitized or confused about the risk (Romanosky et al., 2011; Ponemon, 2014) resulting in a delayed awareness of identity theft. Research currently has ignored examining how long this delayed awareness may last and what these individuals will think and do once they become aware of the identity theft.

Given the increasing probability that individuals will be victims of more than one cyber-breach (Acquisti et al., 2014), there is a research gap in assessing if the individual will be able to attribute the trust and commitment violation to the proper firm. Identity theft victims (in particular delayed awareness victims) may not know who to blame, but blame will be assigned (Ping et al., 2015). Research identifies that some crises can have spillover impacts on similar brands in the industry (Roehm & Tybout, 2006; Lei et al., 2008; Vassilikopoulou et al., 2009; Ping et al., 2015). The attribution of blame generally is reflected in a reduction in trust and a reduction in commitment to the brand (Dahlen & Lange, 2006; Ping et al., 2015). At this point, the research on the spillover effects of product harm crises such as identity theft is still in its infancy (Klein & Dawar, 2004; Ping et al., 2015).

Figure 1 summarizes the conceptual model of this research. This research will provide contributions to close these research gaps and will address the research question of "What factors positively influence the restoration of customer loyalty after identity theft?"

Figure 1. Conceptual Model



Method

This research will use a mixed method approach with an explanatory sequential design (Quantitative – Qualitative) to explore the decision-making dimensions of customer loyalty. The research will be conducted through an interpretive worldview and focus upon the group level analysis of identity theft victims. The attitudinal and behavioral component of the research study will utilize interviews within an emergent, exploratory, inductive study approach (Saldana, 2012). Consistent with an interpretive worldview, the data analysis will use exploratory methods which incorporate the use of attribute, descriptive and pattern coding (Saldana, 2012). In addition, values, emotional and magnitude coding will be used to provide added dimensional insights to the data (Saldana, 2012). Insights will produce categorical themes, propositions and a relevant theoretical model grounded in data from participants which can directly influence strategies, policies, procedures, and future research (Merriam, 2001).

Case Identification

The subject of the research will be a large financial services firm which successfully navigated through a data breach within the prior three years. Given the growth in the number of cyber-breaches and the increasing occurrences of identity theft within the general population, this firm is concerned about the increasing risk of spillover attribution blame negatively impacting its results. As such, it has commissioned this research to gain insights from identity theft victims to assist in evaluating its own customer loyalty program. Alignment has been reached on the explanatory sequential design and the primary research question.

The mixed method research approach will combine qualitative and quantitative methods for data collection and analysis (Creswell, 2012; Creswell & Plano Clark, 2011; Tashakkori & Teddlie, 2003). The quantitative research segment will gather key background insights and demographic information about the general survey sample. It will also allow for the identification of a group of identity theft victims to be solicited for participation in the qualitative segment of the research program. A benefit of using the sequential approach is that the key findings in the quantitative stage will be significantly enhanced and strengthened through the qualitative program stage. In this qualitative stage, interviews will be used to verify and explain the researcher's interpretation of the statistical analysis. Furthermore, the interviews will give an opportunity for the researcher to integrate statistics with thematic data to answer the research questions with credibility.

Quantitative survey

The financial services firm has agreed to participate in this study and will provide access to its customer history files for participant selection. As a result, the researcher has access to a population of prior cyber-breach victims but it is unknown if these individuals actually experienced identity theft. This approach will enable random purposeful sampling (Creswell, 2007, p31).

A field study will be conducted for this stage of the project. The objective of this study is to gather background information on the number of times that the individual has been notified that they were a

victim of any cyber-breach and to confirm the participant's perception that they have been a victim of identity theft on at least one occurrence.

The Company will send the initial solicitation email from the company's email platform to a random purposeful sample of 500 individuals who were customers at the time of the cyber-breach. Respondents will be asked to complete a self-administered survey by logging into a web-based survey tool using the Qualtrics software located on a server within the company's firewall secured network. The survey response period will be 7 days.

The email will advise individuals that the survey is expected to include 30 questions (see Exhibit 1 for the survey questions), will require approximately 15 minutes to complete. The survey will be available for response during the following seven-day period.

The Qualtrics software will anonymize the responses and assign a randomized number schema to preserve the integrity of the data prior to providing access to the researcher. The company's human resource (HR) department will administer the survey and have sole access to the raw survey responses.

Participation will be voluntary and responders will acknowledge and e-sign an informed consent form prior to the beginning of the survey. Participants will be advised that the survey results will be confidential, no one will attempt to contact them to sell products or services and that a summary of the study results will be available to them, if desired, at the conclusion of the study.

Responders who complete the initial entry into the survey tool and completion of the informed consent requirements will receive a $10 e-Certificate regardless of whether they fully complete the survey or not. The company's HR department will administer the distribution of the e-certificates as they are the only group with access to the contact information for each individual.

Qualitative approaches

Participants who complete the quantitative survey and self-disclose that they are an actual identity theft victim will form the population of participants eligible for random selection participation in the qualitative stage. This allows for the utilization of a purposeful sampling approach (Sandelowski, 1995). Participants will be recruited by the financial services company via email and confirmed via telephone for participation in this research stage.

Participants in the qualitative research stage (i.e., those who have completed both the initial registration and informed consent requirements for the qualitative research stage) will receive a $50 American Express gift card for attending the focus group interview. The company's HR department will administer the distribution of the e-certificates as they are the only group with access to contact information for each individual.

Two in-person focus groups and two online structured interview focus groups (Stewart & Williams, 2005) will be held. Each group will consist of 7 – 10 randomly selected self-identified identity theft participants (Creswell, 2007). If the quantity of recruited participants is less than 28, then the number of focus groups will be reduced to no lower than two focus groups containing a minimum of 20 total participants.

The purpose of this qualitative research is to explore the decision-making dimensions of customer loyalty. Data gathering will be conducted from conducting interviews, making observations and collecting documents (Yin, 2013). Both the in-person and the online focus groups will be video-recorded and utilize a professional interviewer (see Exhibit 2 for focus group areas of focus). Web logs will be captured for all online sessions. The combination of in-person interviews and online approaches is intended to reduce biases associated with technology competency as well as enable wider accessibility to geographically dispersed participants.

Data gathering will be conducted through interviews, observations and collection of documents (Yin, 2013) within a forty-five-day period beginning September 15th. Two 2-hour videotaped structured interview focus groups will be held in Dallas on September 15th and 16th. Two online structured interview (see Exhibit 3 for focus group goals and script) focus groups (Stewart & Williams, 2005) will be held on September 17th and 18th. Each group will consist of 7 – 10 participants (Creswell, 2007).

This approach is expected to highlight some conceptual and practical understandings of customer loyalty decision criteria within the real-life context of identity theft victims (Yin, 2013). This exploratory, inductive instrumental study (Stake, 1995) creates opportunities for the researcher to explore additional questions through the act investigating a topic in detail (Hancock & Algozzines, 2006). The embedded analysis will seek common themes that will allow for the creation of propositions for future research (Yin, 2013).

Data analysis

This qualitative study will use exploratory methods which reflect an open-ended investigation and preliminary assignments of codes to the data before more refined coding systems are developed and applied (Saldana, 2012). This method is appropriate as the interview questions are aligned with the research question and generally suggest the exploration of the participants' actions/processes and perceptions found in the data (Saldana, 2012).

The first cycle coding will collect categorical instances from the data using attribute, descriptive and values coding. Attribute coding will be used to identify basic descriptive information such as field setting, participant characteristics or demographics, data format, and other variables of interest for analysis useful for future needs analysis and interpretation involving data management, reference and context (Saldana, 2012). Descriptive coding assigns labels to data to assist in creating categorical themes (Merriam, 2001). Values coding will be used to capture the intrapersonal and interpersonal participant experiences (Saldana, 2012) as well as the perceived strength of the affective relationship between the victim and the provider in terms of trust and commitment (Haelsig et al., 2007).

The second cycle will use eclectic coding to synthesize the variety and number of codes into a more unified scheme (Saldana, 2012). The eclectic coding is then integrated into the use of pattern coding to assign a category label ("meta-code") that identifies similarly coded data (Saldana, 2012. The pattern coding organizes the meta-code into sets, themes, or constructs and attributes meaning to the organization for the development of themes and explanations of the data (Saldana, 2012).

For the scope of this qualitative study, it is likely that a third cycle of coding will be needed. The goal of this cycle is to further enrich the context and insights associated with the themes and observations from the data (Saldana, 2012). This cycle will integrate the pattern coding with the emotional coding and magnitude coding to derive a hierarchy of themes based upon attitudes and beliefs. Emotional coding labels the emotions recalled and/or experienced by the participant, or inferred by the researcher about the participant towards the attribution of blame (Ping et al., 2015) and the feelings of betrayal associated with the reduction in trust (Dahlen & Lange, 2006; Ping et al, 2015) experienced by these same individuals. Magnitude coding will add an intensity context to the output as well as assist in identifying significant quotes (Saldana, 2012).

Biases

The following items represent possible limitations that might be applicable to this consumer-based survey. Non-response bias. The findings are based on a sample of survey returns. Sampling-frame bias. The sample results may be biased by external events such as recent media coverage. Because a web-based collection method will be used, it is possible that non-web responses would have resulted in a different pattern of findings. Self-reported results. The quality of survey research is based on the responder's perception of the question and may or may not reflect the actual experience. To minimize the potential impact of these biases, various quantitative techniques (e.g., Crombach ∞ and Confirmatory Factor Analysis) will be used to evaluate the magnitude of certain biases within the study data and results. In addition, these potential biases will be analyzed by comparing the respondent-based estimates with those from another, more accurate source. The quantitative survey contains various demographic elements which will enable the comparison of the distributions of age, gender, race, and other sociodemographic variables among respondents with those from the most recent census data for the population.

Ethical considerations

The proposal will be approved by the university's institutional review board as well as the financial services firm's human resource and legal organizations. Given the deeply personal and sensitive nature of the customer loyalty and data privacy intrusions, the rights of the participants must be

protected and respected. Similarly, the firm's brand must not incur further damage as a result of this study.

Participation will be voluntary and responders will acknowledge and e-sign an informed consent form prior to the beginning of the survey. Participants will be advised that the survey results will be confidential, no one will attempt to contact them to sell products or services and that a summary of the study results will be available to them at the conclusion of the study.

The questionnaire will seek participant identification of any cultural, religious, gender or any other differences that need special attention and respect. It will also confirm that all participants are at least 18 years of age or older. All collected data will be anonymized, and the identity of the participants and firm will be protected. All personally identifiable information will be available only to the company's HR department, and even then only for use in providing remuneration for participation. This group will also assign the anonymous codes for each account. Except for the HR group, no one in the firm nor anyone on the research team will have access to personally identifiable information, place of employment or participant-specific demographic profiles. In addition, no actual credit card purchase documents, monthly statements, user ids or passwords will be accepted.

Discussion and implications

The purpose of this research is to address research gaps associated with identifying the relevant and important decision-making attitudes and behavioral processes associated with incentivizing customer loyalty for victims of identity theft. Extant literature has identified four primary background themes impacting this study. First, customer loyalty is import to the financial success of the company. Second, loyalty programs assist in deepening the affective relational bond with the company which proves beneficial in regaining customer trust after a service recovery incident. Third, identity theft victims may not know who to blame for the trust and commitment breach but blame will be assigned. Lastly, spillover blame attribution can be experience by companies not directly involved in the cyber-breach which led to the victim's identity theft incident.

These background themes are important because of the direct relationship to efforts to establish a perception of a trustful and deeply loyal relationship with the customer. This loyalty will assist in maintaining a consistent pipeline for revenues while lowering customer acquisition costs and yielding increased profits. Additional benefits include an increase in the customer's perception of brand equity as well as a possible deterrent to large liability litigation for damages from a cyber-breach.

The implications of identity theft are very personal to each victim. The mixed method approach uses an explanatory sequential design to explore the decision-making dimensions of customer loyalty. This mixed method approach allows for richer insights to be captured and identified from the data collected from the identity theft victim case study. The representative sample consists of self-identified identity theft victims who were also victims of a prior cyber-breach at a financial services firm. The multiple methods of collecting data and the multiple approaches for analyzing the data, provide truth value, applicability, consistency and authenticity for the outcome results.

These insights answer the investigative questions and answer the research question, "What factors positively influence the restoration of customer loyalty after identity theft?"

Future research

This study will provide several avenues for further research. First, the study outcome should produce relevant propositions for inclusion in future research intended to explain the impact of identity theft upon the impacts of loyalty decision-making for identity theft victims.
Second, identify the most effective responses to recovering trust after a breach. Third, understand why these people are willing to continue to do business with the firm. Fourth, understand if the perception of company response remedies is significantly different depending upon the severity of the identity theft injury. Fifth, validated model constructs can be incorporated into a longitudinal study to explore unique time-dimensional impacts associated with loyalty decision-making for identity theft victims. Sixth, the research can be expanded to include additional cases. Lastly, the research insights will enable a future mixed method study focused upon new concepts for identity wellness tools which

will provide tangible additional incentive benefits and value to identity theft victims as a loyalty enhancer.

Expected outcomes

Expected outcome themes include victims' perception of trust and loyalty towards companies that help protect them from future impacts and injuries associated with identity theft. The perceived impacts of identity theft vary by victim. Severe cases can produce large personal financial injury and high levels of negative emotional involvement. These injuries fracture trusting relationships and contribute to victim use of wide-broadcast blame attribution among many companies. However, in times of uncertainty, customers are expected to align with their established provider relationships or with generally recognized reputable brands.

As new technology emerges, victims will value insights from reputable companies which can assist the victims in their fight against additional identity theft injury. Companies which offer identity wellness tools which are embraced by customers are expected to realize enhanced brand loyalty. This enhanced loyalty might assist companies in their defense against litigation or new legislative actions which might impose requirements for companies to invest in expensive protection remedies for identity theft victims.

This research is important because it addresses certain research gaps, establishes a roadmap for future research and enables organizations that use this research to assess and design new loyalty programs, evaluate new identity wellness tools and assess risks associated with the increasing possibility of spillover blame impacts being attributed to their company.

References

Acquisti, A., Taylor, C., & Wagman, L. (2014). The economics of privacy. *Journal of Economic Literature*.

Archer, N., Sproule, S., Yuan, Y., Guo, K., & Xiang, J. (2012). *Identity Theft and Fraud: Evaluating and Managing Risk*. University of Ottawa Press.

Bateman, T. S., & Organ, D. W. (1983). Job satisfaction and the good soldier: The relationship between affect and employee "citizenship". *Academy of management Journal*, *26*(4), 587-595.

Benton, M., Blair, K., Crowe, M. D., & Schuh, S. D. (2007). The Boston Fed study of consumer behavior and payment choice: a survey of Federal Reserve System employees. *FRB of Boston Public Policy Discussion Paper*, (07-1).

Boshoff, C. (2005). A re-assessment and refinement of RECOVSAT: An instrument to measure satisfaction with transaction-specific service recovery. *Managing Service Quality: An International Journal*, *15*(5), 410-425.

Brill, J. (2014). Internet of Things: Building Trust and Maximizing Benefits through Consumer Control, The. *Fordham L. Rev.*, *83*, 205.

Burns, P., & Stanley, A. (2002). Fraud management in the credit card industry. *Federal Reserve Bank of Philla Payment Cards Center Discussion Paper*, (02-05).

Chen, M., Chen, C., & Farn, C. (2010). EXPLORING DETERMINANTS OF CITIZENSHIP BEHAVIOR ON VIRTUAL COMMUNITIES OF CONSUMPTION: THE PERSPECTIVE OF SOCIAL EXCHANGE THEORY. *International Journal of Electronic Business Management, 8*(3), 195-205.

Chicago Tribune (2015). Hackers stole Social Security numbers from 21 million in data breach. Accessed July 10, 2015 at http://www.chicagotribune.com/news/nationworld/ct-social-security-numbers-data-breach-20150709-story.html

Cho, Y. C., & Song, J. (2012). The Effects Of Customer Dissatisfaction On Switching Behavior In The Service Sector. *Journal of Business & Economics Research (JBER)*, *10*(10), 579-592.

Cohen, P. (2015). I.R.S. data breach may be sign of more personalized schemes, *The new york time*s, Accessed June 25, 2015 at http://www.nytimes.com/2015/05/28/business/irs-data-breach-may-be-sign-of-more-personalized-schemes.html?_r=0

Cleeren, K., Dekimpe, M.G. and Helsen, K. (2006), *Weathering Product-harm Crises*, Department of Marketing and Organisation Studies (MO), Katholieke Universiteit Leuven, Leuven, pp. 262-70.

Conger, S. (2015). Qualitative Methods for Diagnosis and Assessment. *University of Dallas*. As accessed on August 13, 2015 from http://imba.udallas.edu/re/DotNextLaunch.asp?courseid=11537461&userid=27902055&sessionid=e54fdb4498&tabid=oqQZjzMovCrOXCNQaSCj84J+OaxMA6KTXsHlmPXIaLJn6avTlbE8Bln6l1xQAzLNHhQDnK+ChsQKP25KPCjk9w==&sessionFirstAuthStore=true&macid=b08L4lGhfDFzpMFJC8elRYNA5jCxvtHV/hcrAtCMDXALSYBVzhRDVsFNnNBGDcauvXYKtjL9snk2lSYfvUNFMeX1gXnqOD/6kdecwJkO9Cofu9LR7GMlPaEQHZ5PSzRpJPzWo5hBbcBlJ4awPvick+TPNrpzBgMYGLfL7wsj7Yj7mkou+U6r+wweAG82bzwcrvL6ySYtc4Y+oLRy8DYpIoAv721VR69I1TvYlNYmsQ/9F65EAeV4CPkz9S2P/Td7

Copes, H., Kerley, K. R., Huff, R., & Kane, J. (2010). Differentiating identity theft: An exploratory study of victims using a national victimization survey. *Journal of Criminal Justice*, *38*(5), 1045-1052.

Creswell, J. W. (2007). Qualitative inquiry and research method: Choosing among five approaches.

Creswell, J. W. (2012). *Qualitative inquiry and research design: Choosing among five approaches*. Sage.

Creswell, J. W., & Plano Clark, V. L. (2011). Collecting data in mixed methods research. *Designing and conducting mixed methods research. 2nd ed. Thousand Oaks: SAGE Publications*, 171-202.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. *Mis Quarterly*, 673-687.

Dahlen, M. & Lange, F. (2006) A disaster is contagious: how a brand in crisis affects other brands. *Journal of Advertising Research*, **46**, 4, pp. 388–397.

Datacandy.com, (2014). Accessed on June 8, 2015 at https://www.datacandy.com/resources/blog/blog-post-b

Davcik, N. S., Vinhas, d. S., & Hair, J. F. (2015). Towards a unified theory of brand equity: Conceptualizations, taxonomy and avenues for future research. *The Journal of Product and Brand Management, 24*(1), 3-17.

Dawar, N., & Lei, J. (2009). Brand crises: The roles of brand familiarity and crisis relevance in determining the impact on brand evaluations. *Journal of Business Research*, *62*(4), 509-516.

Dawar, N., & Pillutla, M. M. (2000). Impact of product-harm crises on brand equity: The moderating role of consumer expectations. *Journal of Marketing Research*, *37*(2), 215-226.

D'Souza, G., & Phelps, J. E. (2009). The privacy paradox: The case of secondary disclosure. *Review of Marketing Science*, *7*(1).

Eisenstein, E. M. (2008). Identity theft: an exploratory study with implications for marketers. *Journal of Business Research*, *61*(11), 1160-1172.

Eisner, E. W. (1991). *The enlightened eye: Qualitative inquiry and the enhancement of educational practice*. Prentice Hall.

Ely, M., Anzul, M., Friedman, T., Garner, D. & Steimnetz, A. (1991). *Doing qualitative research: Circles within circles*. New York: Falmer Press.

Erlandson, D. A. (1993). *Doing naturalistic inquiry: A guide to methods*. Sage.

Evanschitzky, H., Ramaseshan, B., Woisetschläger, D. M., Richelsen, V., Blut, M., & Backhaus, C. (2012). Consequences of customer loyalty to the loyalty program and to the company. *Journal of the Academy of Marketing Science*, *40*(5), 625-638.

Fornell, C., & Wernerfelt, B. (1987). Defensive marketing strategy by customer complaint management: a theoretical analysis. *Journal of Marketing research*, 337-346.

Glesne, C., & Peshkin, A. (1992). *Becoming qualitative researchers: An introduction* (p. 6). White Plains, NY: Longman.

Goss, R. J., Silvera, D. H., Laufer, D., Gillespie, K., & Arsena, A. (2011). Uh-oh, this might hurt our bottom line: consumer and company reactions to product harm crises. *Journal of Consumer Research*, *35*(6), 985-1002.

Guba, E. G. (1979). Naturalistic inquiry. *Improving Human Performance Quarterly*, *8*(4), 268-76.

Haelsig, F., Swoboda, B., Morschett, D., & Schramm-Klein, H. (2007). An intersector analysis of the relevance of service in building a strong retail brand. *Managing Service Quality*, 17(4), 428-448.

Hancock, D. R., & Algozzine, B. (2006). *Doing case study research: A practical guide for beginning researchers*. Teachers College Press.

Huseman, R. C., Hatfield, J. D., & Miles, E. W. (1987). A new perspective on equity theory: The equity sensitivity construct. *Academy of management Review*, *12*(2), 222-234.

Kahn, C. M., & Liñares-Zegarra, J. M. (2012). Identity theft and consumer payment choice: Does security really matter?. *Journal of Financial Services Research*, 1-39.

King-Casas, B., Sharp, C., Lomax-Bream, L., Lohrenz, T., Fonagy, P., & Montague, P. R. (2008). The rupture and repair of cooperation in borderline personality disorder. *science*, *321*(5890), 806-810.

Klein, J., & Dawar, N. (2004). Corporate social responsibility and consumers' attributions and brand evaluations in a product–harm crisis. *International Journal of research in Marketing*, *21*(3), 203-217.

Laufer, D., & Gillespie, K. (2004). Differences in consumer attributions of blame between men and women: The role of perceived vulnerability and empathic concern. *Psychology & Marketing*, *21*(2), 141-157.

LeCompte, M. D., & Goetz, J. P. (1982). Problems of reliability and validity in ethnographic research. *Review of educational research*, *52*(1), 31-60.

Lee, J., Lee, J., & Feick, L. (2001). The impact of switching costs on the customer satisfaction-loyalty link: mobile phone service in France. *Journal of services marketing*, *15*(1), 35-48.

Lei, J., Dawar, N., & Lemmink, J. (2008). Negative spillover in brand portfolios: exploring the antecedents of asymmetric effects. *Journal of marketing*, *72*(3), 111-123.

Li, M. L., & Green, R. D. (2011). A mediating influence on customer loyalty: The role of perceived value. *Journal of Management and Marketing Research*, *7*(1), 1-12.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry* (Vol. 75). Sage.

Ma, B., Zhang, L., Wang, G., & Li, F. (2014). The impact of a product-harm crisis on customer perceived value. *International Journal of Market Research*, *56*(3), 341-366.

Malhotra, A., & Malhotra, C. K. (2010). Evaluating customer information breaches as service failures: an event study approach. *Journal of Service Research*, 1094670510383409.

Martin, K., & Parmar, B. (2012). Assumptions in decision making scholarship: Implications for business ethics research. *Journal of business ethics*, *105*(3), 289-306.

Merriam, S. (2001). B.(1988). Case study research in education: A qualitative approach.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage.

Milne, G. R., Boza, M. E., & Rohm, A. (1999, January). Controlling personal information in marketing databases: a consumer perspective. In *American Marketing Association. Conference Proceedings* (Vol. 10, p. 107). American Marketing Association.

Milne, G. R., Gabisch, J. A., Markos, E., & Phelps, J. E. (2012). Changes in Consumer Willingness to Provide Information over the Last Decade: A Cohort Analysis. *International Journal of Integrated Marketing Communications*, *4*(2).

Milne, G. R., & Rohm, A. J. (2000). Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives. *Journal of Public Policy & Marketing*, *19*(2), 238-249.

Mowen, J. C. (1980). Further information on consumer perceptions of product recalls. *Advances in Consumer Research*, *7*(1), 519-523.

Nash, K. (2015). Appeals court revives Neiman Marcus data breach suit. *The Wall Street Journal*. As accessed on August 12, 2015 at http://blogs.wsj.com/cio/2015/07/23/appeals-court-revives-neiman-marcus-data-breach-suit/.

Newman, G. R., & McNally, M. M. (2005). Identity theft literature review. *United States Department of Justice: National Institute of Justice*.

Norberg, P. A., & Horne, D. R. (2007). Privacy attitudes and privacy-related behavior. *Psychology & Marketing*, *24*(10), 829-847.

Oly Ndubisi, N. (2006). Effect of gender on customer loyalty: a relationship marketing approach. *Marketing Intelligence & Planning*, *24*(1), 48-61.

Pagliery, J. (2015). CNNMoney.com. http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/?iid=EL. Accessed on June 23, 2015.

Papadakis, I. S. (2006). Financial performance of supply chains after disruptions: an event study. *Supply Chain Management: An International Journal*, *11*(1), 25-33.

Peltier, J. W., Milne, G. R., & Phelps, J. E. (2009). Information privacy research: Framework for integrating multiple publics, information channels, and responses. *Journal of Interactive Marketing*, *23*(2), 191-205.

Petriglieri, J. L. (2015). Co-creating Relationship Repair Pathways to Reconstructing Destabilized Organizational Identification. *Administrative Science Quarterly*, 0001839215579234.

Phelps, J. E., & Milne, G. R. (2009). Integrated marketing communications and new media: Emerging privacy issues. *International Journal of Integrated Marketing Communications*, *1*(1), 84-93.

Ping, Q., Ishaq, M., & Li, C. (2015). Product Harm Crisis, Attribution of Blame and Decision Making: An Insight from the Past. *J. Appl. Environ. Biol. Sci*, *5*(5), 35-44.

Ponemon Institute. 2014. The Aftermath of a Data Breach: Consumer Sentiment. Retrieved from http://www.ponemon.org/library/the-aftermath-of-a-data-breach-consumer-sentiment?s=the+aftermath+of+a+data+breach on June 5, 2015.

Pruitt, S. W., & Peterson, D. R. (1986). Security price reactions around product recall announcements. *Journal of Financial Research*, *9*(2), 113-122.

Reichheld, F. F., & Schefter, P. (2000). E-loyalty. *Harvard business review*, *78*(4), 105-113.

Rempel, J. K., Holmes, J. G., & Zanna, M. P. (1985). Trust in close relationships. *Journal of personality and social psychology*, *49*(1), 95.

Roehm, M. L., & Tybout, A. M. (2006). When will a brand scandal spill over, and how should competitors respond? *JMR, Journal of Marketing Research*, *43*(3), 14.

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft?. *Journal of Policy Analysis and Management*, *30*(2), 256-286.

SafeNet, (2014). Global Survey Reveals Impact of Data Breaches on Customer Loyalty. Accessed July 1, 2015 at http://www.safenet-inc.com/news/2014/data-breaches-impact-on-customer-loyalty-survey/

Saldaña, J. (2012). *The coding manual for qualitative researchers* (No. 14). Sage.Sandelowski, M. (1995). Sample size in qualitative research. *Research in nursing & health*, *18*(2), 179-183.

Schilke, O., Reimann, M., & Cook, K. S. (2013). Effect of relationship experience on trust recovery following a breach. Proceedings of the National Academy of Sciences, 110(38), 15236-15241

Shinal, J. (2015, June 16). Medical-device, IoT hacks spurring security software boom, *USATODAY*. http://www.usatoday.com/story/tech/columnist/shinal/2015/06/16/medical-device-hacks-john-shinal-new-tech-economy/28782173/

Silverman, D. (2006). *Interpreting qualitative data: Methods for analyzing talk, text and interaction*. Sage.

Siomkos, G. J. (1999). On achieving exoneration after a product safety industrial crisis. *Journal of Business & Industrial Marketing*, *14*(1), 17-29.

Siomkos, G. J., & Kurzbard, G. (1994). The hidden crisis in product-harm crisis management. *European journal of marketing*, *28*(2), 30-41.

Siomkos, G. J., & Malliaris, P. G. (2011). Consumer response to company communications during a product harm crisis. *Journal of Applied Business Research (JABR)*, *8*(4), 59-65.

Smith, J., & Hart, P. (2011). n for Info. *Journal of the Association for Information Systems*, *12*(12), 798-824.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania law review*, 477-564.

Stake, R. E. (1995). *The art of case study research*. Sage.

Steinhoff, L., & Palmatier, R. W. (2014). Understanding loyalty program effectiveness: managing target and bystander effects. *Journal of the Academy of Marketing Science*, 1-20.

Stewart, K., & Williams, M. (2005). Researching online populations: the use of online focus groups for social research. *Qualitative Research*, *5*(4), 395-416.

Tashakkori, A., & Teddlie, C. (2003). Issues and dilemmas in teaching research methods courses in social and behavioural sciences: US perspective. *International Journal of Social Research Methodology*, *6*(1), 61-77.

Teddlie, C., & Tashakkori, A. (2003). Major issues and controversies in the use of mixed methods in the social and behavioral sciences. *Handbook of mixed methods in social & behavioral research*, 3-50.

Tsang, E. W. (2000). Transaction cost and resource-based explanations of joint ventures: A comparison and synthesis. *Organization studies*, *21*(1), 215-242.

Urban, G. L., Sultan, F., & Qualls, W. J. (2000). Placing trust at the center of your Internet strategy. *Sloan Management Review*, *42*(1), 39-48.

Vassilikopoulou, A., Siomkos, G., Chatzipanagiotou, K., & Pantouvakis, A. (2009). Product-harm crisis management: Time heals all wounds?. *Journal of Retailing and Consumer Services*, *16*(3), 174-180.

Wang, K., Hsu, L., & Chih, W. (2014). Retaining customers after service failure recoveries: A contingency model. *Managing Service Quality*, *24*(4), 318.

Xia, L., & Kukar-Kinney, M. (2014). For our valued customers only: Examining consumer responses to preferential treatment practices. *Journal of Business Research*, *67*(11), 2368-2375.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: toward an integrative view. *ICIS 2008 Proceedings*, 6.

Yang, Z., & Peterson, R. T. (2004). Customer perceived value, satisfaction, and loyalty: The role of switching costs. *Psychology & Marketing*, *21*(10), 799-822.

Yin, R. K. (2013). *Case study research: Design and methods*. Sage publications.

Appendix

Exhibit 1

Quantitative Survey

Survey	Selection				
Please select the one best answer that reflects your knowledge or understanding of the situation by clicking on the appropriate button. As a reminder, all responses are confidential and anonymous. Results will be summarized. No one will attempt to contact you to sell you a product or service. (These questions are a sample of the demographic questions.)					
1. Has any organization ever notified you about a data breach that involved your personal information?	Yes	No			
	○	○			
2. How many data breach notifications as described above, representing different incidents, have you received in the past 2 years?	1	2	3	4	5 or more
	○	○	○	○	○
3. In regards to the latest notification that you received within the last two years, how did you react? (Please check one response only.)	Ignored it	Followed the advice	Seek more information		
	○	○	○		
4. Did any of the notifications offer identity theft protection?	Yes	No			
	○	○			
5. Prior to the data breach(s), how concerned were you that you would become an identity theft victim?	Extremely Concerned	Very Concerned	Neutral	Somewhat Concerned	Not Concerned
	○	○	○	○	○
6. Following the data breach(s), how concerned are you that you will now become an identity theft victim?	Extremely Concerned	Very Concerned	Neutral	Somewhat Concerned	Not Concerned
	○	○	○	○	○
7. Within the past 2 years, have you become a victim of identity theft?	Yes	No			
	○	○			
8. What steps have you taken to protect yourself against identity theft? (Check as many as appropriate.)	Cancelled credit/debit card	Enrolled in Identity Theft Protection Program	Monitor Credit Report Regularly	Hired an Attorney	Nothing
	○	○	○	○	○
9. How long did it take to resolve the consequences of the breach?	1 month	3 months	6 – 12 months	1 – 2 years	Not resolved
	○	○	○	○	○
10. Did you discontinue your relationship with the company after the data breach?	Yes	No			
	○	○			
11. If you continued your relationship with the company after the data breach, why did you do so?	Too Much Time to Find Another Provider	The Company Resolved My Concerns	The Quality and Price Meet My Needs	Every Company Is Getting Hacked	Other
	○	○	○	○	○
The following questions are intended to gather some general information about yourself. (These questions are a sample of the demographic questions.)					
12. Identify your gender.	Male	Female			
	○	○			
13. Identify your marital status.	Single	Married			
	○	○			

Exhibit 1

Quantitative Survey

Survey	Selection				
14. Select the group that best represents your current age.	18 - 34	35 - 44	45 - 54	55+	Other
	○	○	○	○	○
15. Select the highest level of education completed.	Less than high school	High school graduate	Some college	College graduate	Post-graduate studies
	○	○	○	○	○
16. Identify your current annual income.	Less than $25,000	$25,000 to $50,000	$50,000 to $80,000	$80,000 - $120,000	Above $120,000
	○	○	○	○	○

Coding notes:

- Gender: Male = 1, Female = 2
- Marital Status: Single – 1, Married = 2
- Age: 18 to 29 = 1, 30 to 39 = 2, 40 to 49 = 3, 50+ = 4, Other = 5
- Education: < than high school = 1, high school = 2, some college = 3, college graduate = 4, post-graduate =5
- Income: < $25,000 = 1, $25,000 to $50,000 = 2, $50,000 to $80,000 = 3, $80,000 - $120,000 = 4, Above $120,000 = 5

The survey is expected to include 30 questions and require 15 minutes to complete.

Exhibit 2

Data Collection Matrix

Focus Group	Probes
IQ #1	1. How did you discover that your identity had been stolen? a. How do you think that your identity was stolen? b. What actions did you take once you found out that your identity had been stolen? c. Was any assistance offered to you by the cyber-breached company?
IQ #2	2. Do you blame anyone or any company for your identity theft? a. Have you shopped or purchased goods from that company again? b. What are your privacy expectations for a business that you want to shop with? c. How do you monitor your purchasing history or credit rating?
IQ #3	3. What factors do you rank highly in a company that you are loyal to? a. What are the top criteria influencing your decision to be loyal to a company? b. Do you get recommendations from family or friends? c. Name some of the most trusted companies to do business with? d. Do you talk about your experiences to others?
IQ #4	4. Have you changed your shopping behavior? a. Do you buy from all the same companies as you did prior to the cyber breach? b. Do you pay for things the same way? c. Do you provide your personal information when asked? d. Do you read privacy policies?

Exhibit 3

Interview Script

Section	Probes
Introduction (10 min.)	*Objectives: Warm up respondents, explain tasks, reassure and create comfortable atmosphere, encourage involvement* • Thank respondents for participating; introduce self (interviewer) and purpose of research • Go over rules for the session – explain recording (videotape), confidentiality, not to take calls on the mobile, make themselves feel at home/ get comfortable • Review Goals – to understand how you feel about customer loyalty after identity theft. There are no right or wrong answers, whatever you feel and the impressions you have. • Explain that we want to encourage an open mind-set, start with asking respondents to introduce themselves, what they do for a living, household composition, etc.
Section #2 (15 min.)	*Goal: Establish a baseline relationship with the participants on the impacts of credit card fraud.* • How many times have you been a victim of credit card fraud in the last year? • How did you find out about the credit card fraud? • How did you feel once you found out about the credit card fraud? • Was it easy to get the fraudulent charges removed from your account? • Have you changed how you shop since you found out about the credit card fraud? • Who do you blame for the credit card fraud?
Section #3 (15 min.)	*Goal: Identify participant awareness and responsiveness to cyber-breach notifications.* • Has any organization ever notified you about a cyber-breach that involved your personal information? • Have you received a notification from the Internal Revenue Bureau that you have been a victim of a cyber-breach? • Have you received a notification from a Credit Bureau that you have been a victim of a cyber-breach? • Have you received a notification from a medical insurance company that you have been a victim of a cyber-breach? • How did you feel once you received any notification that you have become a victim of a cyber-breach? • Did you take any actions after receiving the notification? • Do these notifications provide helpful recommendations on protecting your personal information? • How can these notifications be improved for provide assistance to you?
Section #4 (20 min.)	*Goal: Identity how identity theft has impacted their life.* • Since each of you is an identity theft victim, what challenges has it introduced to your life? • Was it difficult to remedy the impacts of the identity theft? • How long did it take to resolve the consequences of the identity theft? • Are there any consequences of the identity theft which have not yet been resolved?
Section #5 (20 min.)	*Goal: Identify blame attribution.* • Do you blame anyone for your identity theft? • Do you know who to blame for your identity theft?

Exhibit 3

Interview Script

Section	Probes
	• Are you suspicious of another company because they are similar to the company that you blame for your identity theft? • Do you blame any company even though you are not positive that they were involved in your identity theft?
Section #6 (20 min.)	Goal: Focus the mindset to a more positive tone. Identify customer loyalty attributes. • Name your top three companies that you are loyal to. • Why do you feel loyal to them? • Do they offer programs that make you feel special to them? • Are you primarily loyal to the company because of the special incentives? • If any of these top three companies notified you that you have become a cyber-breach victim, would you still feel loyal to them?
Section #7 (10 min.)	*Goal: Identify suggestions for new programs or tools to assist identity theft victims.* • What new program or tool could be created to provide better assistance to identity theft victims? • If a company other than your three favorites offered you this special program or tool, would you do business with this company? • Should the government mandate special assistance programs to identity theft victims?
Wrap-up (10 min.)	• Check with research observers for other questions. • Remind participants that the $50 American Express gift card will be mailed to the address that they provided in response to the recruitment email. The cards should arrive within 10 – 14 days. • Provide each participant with a card including the focus group date, reference code and contact information if there are questions about the gift card. • Thank each individual for their participation!