Identity Theft, Mistrust, and the Production of Economic Insecurity

Jordan Brensinger
Princeton University

Abstract
Across various domains of social life, organizational reliance on personal data and exposure to unanticipated hardship have transformed Americans' life chances and access to opportunities. This article examines an area where they intersect: the hardship caused by breakdowns in information systems. I focus on the case of identity theft, showing how that event—experienced by millions of Americans annually—constitutes an overlooked source of economic insecurity. I develop a theory of insecurity that links feelings of precariousness to breaches of trust at three levels: interpersonal, organizational, and systemic. Drawing on an original qualitative study of identity theft resolution, I find that most victims worried about their financial lives because they could no longer count on certain actors or systems. Beneath this commonality, race and class informed feelings of insecurity and associated coping strategies following identity theft. Low-income people and people of color tended to direct suspicion at personal networks and report ending relationships and informal assistance. In contrast, middle- and upper-income individuals and whites disproportionately blamed organizations and demanded their protection. These findings—along with the trust-based theory that helped make them visible—have important implications for the study of insecurity, inequality, and trust in the information age.

Keywords
personal data, risk, trust, inequality, identity theft

Introduction
Since the 1970s, two trends have steadily transformed Americans' livelihoods: organizational reliance on personal data[1] for individualized decision-making and growing insecurity resulting from exposure to unanticipated events. With respect to the importance of personal data (Bouk 2017; Fourcade and Healy 2017), credit scores and reports offer a paradigmatic example. Financial institutions, landlords, and employers widely consider them when evaluating consumers for a multitude of resources and opportunities including credit, insurance, housing, and employment (Kiviat 2019a; Rona-Tas 2017; Rosen, Garboden, and Cossyleon 2021). Alongside the rise of personal data, policies of deregulation in favor of market-based solutions to social welfare leave individuals increasingly vulnerable to hardship caused by unpredictable events like job loss, relationship dissolution, and illness (Western et al. 2012).

These two trends have inspired growing respective bodies of research, yet a key area where they intersect—the hardship caused by breakdowns in information systems—has received far less attention. Although information systems can break down in various ways, this article focuses on one pervasive and salient such event: financial identity theft, defined as when "someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception ... for economic gain" (United States Department of Justice 2017). Conservative estimates place the annual rate of victimization at over 5% of American adults (Tedder and Buzzard 2020), with others locating that rate as high as 20% (Pew Research Center 2019:10). At a minimum, these figures translate into tens of millions of victims each year. Moreover, identity theft speaks directly to the breakdown of information systems in a wide variety of domains, with cases varyingly implicating consumer banking; insurance; housing and utilities; government services (e.g., taxation, welfare); healthcare; and the criminal justice system.

Existing research demonstrates that identity theft can profoundly impact individual wellbeing and access to opportunity. Victims frequently report a range of financial harms, including direct financial losses, unanticipated debt, and inaccurate credit reports (Anderson, Durbin, and Salinger 2008; Harrell 2019), along with emotional and physical difficulties like anxiety, back pain, and difficulty sleeping (Golladay and Holtfreter 2017; Randa and Reyns 2019; Sharp et al. 2004). This body of work helpfully draws attention to the financial and nonfinancial harms associated with identity theft. Yet due to a near exclusive reliance on surveys (but see Greene 2021), it treats these harms as "symptoms" or consequences of a determinate event rather than part of a complex experience and associated process of meaning-making. Consequently, we know relatively little about the rich and varied ways that individuals qualitatively make sense of identity theft, particularly with respect to their ongoing financial lives and welfare.

This article identifies identity theft as an overlooked source of economic insecurity, "the risk of economic loss faced by workers and households as they encounter the unpredictable events of social life" (Western et al. 2012:342). At a time when personal data shapes access to countless consequential resources and opportunities, identity theft and the vulnerability of data it epitomizes can cast a considerable shadow over individuals' financial lives. To account for this, I develop a theory of insecurity that centers the role of trust breaches in experiences of and responses to precarity. Central to this theory, I conceptualize individual trust as comprised of three distinct levels: *interpersonal*, *organizational*, and *systemic*. Perceptions of economic security, that is, hinge on individuals' confidence in the reliability of other people, organizations, or larger systems on which their financial lives depend.

To shed light on individuals' experiences of and responses to identity theft, I draw on an original qualitative study of identity theft resolution. I find that, despite varying levels of material hardship, most victims worried about how they would pay the bills or achieve goals like buying a home because they could no longer trust certain actors or systems to have their backs. Yet race and class informed the nature of their mistrust and associated coping strategies. Low-income people and people of color experienced identity theft as a violation of interpersonal trust: personal information came to appear like a source of vulnerability that opportunistic family, friends, and acquaintances might exploit. In response, they often reported severing relationships and channels of informal assistance to protect themselves. Middle- and upper-income individuals and whites, however, directed disproportionate mistrust toward organizations and demanded their protection. These findings—along with the novel trust-based theory that helped make them visible—have important implications for the study of insecurity, inequality, and trust in the information age.

THE GROWING IMPORTANCE OF PERSONAL DATA

While organizations have long collected and utilized personal data, the 1970s arguably ushered in a new period oriented toward the personalized management of individuals (Bouk 2017). Until that point, personal data primarily facilitated the production of collective abstractions or efforts to situate individuals within some "mass society." The perceived value of that data derived from its usefulness for aggregate analyses rather than anything it said about particular individuals.

Economic, political, and technical developments in the 1970s contributed to transforming that approach. Economic crises motivated organizations to find more cost-effective ways to target advertising or interventions (Bouk 2017). Social movements criticized the biases in human decision-making processes, spurring on quantified risk management with its apparent "objectivity" (Krippner 2017; also see Porter 1996). At the same time, computerization decreased the cost of information storage and enabled new forms of data sharing and analysis (Lauer 2017). These forces propelled the construction of increasingly detailed "data doubles," virtual representations of individuals used in organizational practice (Poster 1990; also see Haggerty and Ericson 2000). Businesses and government agencies now rely on data doubles to identify individuals and evaluate them for a myriad of purposes including calculating crime and child abuse risks, tracking immigration and educational statuses, and allocating resources like credit, healthcare, housing, and public benefits (Brensinger and Eyal 2021; Eubanks 2018; Kiviat 2019a; Lageson 2020; Rosen et al. 2021). Individual wellbeing and access to opportunity depend to a growing extent on personal data.

One important consequence of this trend is that personal data has become increasingly vulnerable to compromise and misuse. The regular and wide circulation of personal data generates opportunities for misappropriation (Marron 2008; Solove 2002), an outcome incentivized by linking that information to all the high-value benefits described above. To address this vulnerability, organizations resort to identification systems that involve checking physical cards, scanning biometrics, analyzing computer metadata, and other techniques (Brensinger and Eyal 2021). The financial industry in particular has invested heavily in anti-fraud systems aimed at limiting unauthorized access to credit and other financial resources (Gates 2010).

Yet government and industry do not bear this burden alone. When it comes to personal data, "institutions are divesting themselves of responsibility for the full social and economic costs of the risks that they have produced" (Whitson and Haggerty 2008:591; also see Monahan 2010). Businesses often prioritize profit over data security (Trost 2017), such as by approving credit requests with misspelled or incorrect information (Hoofnagle 2009). Regulators assign certain responsibilities—often framed as "rights"—to individuals with respect to data management (Solove 2012; Viljoen 2021). The media, law enforcement, and industry also commonly depict

personal data as vulnerable while constructing personal discipline and security-related consumption as moral imperatives (Draper 2019; Gates 2010; Whitson and Haggerty 2008). Together, these factors highlight how contemporary information capitalism in the United States privileges commerce over consumer welfare, leaving individuals to look out for themselves and their associated data (Marron 2008; Trost 2017).

RISING ECONOMIC INSECURITY

This societal approach to personal data conforms to the wider political trend of shifting risk onto individuals. In response to the same social and fiscal crises underlying the organizational turn to personalized decision-making, policymakers in the 1970s began steadily defunding public programs and deregulating industry in favor of private solutions to social problems (Cooper 2014; Krippner 2012). Personal responsibility and consumption quickly replaced social insurance, leaving individuals vulnerable to unexpected economic hardship resulting from sources ranging from precarious employment relationships (Hollister 2011; Kalleberg 2018) and rising healthcare costs (Himmelstein et al. 2009; Houle and Keene 2015) to housing instability (Desmond 2012b; Sullivan 2018) and complex, often exploitative credit relationships (Dwyer 2018). Increased risk in a growing number of domains exposes Americans—particularly low-income people and people of color—to the harsh vicissitudes of economic life.

While not explicitly framed in terms of economic insecurity, an emergent line of scholarship points to how inaccurate data (of which identity theft is one potential cause) can similarly compromise access to critical resources. Inaccuracies in credit reports impact credit access and terms (Wu et al. 2019). Flawed digital criminal records undermine perceived employability and creditworthiness (Lageson 2020). Errors in government eligibility databases lead to denial for public benefits (Eubanks 2018). And faulty tenant screening reports hinder efforts to obtain housing (Kirchner and Goldstein 2020). What's more, low-income individuals may suffer greater harm because they often lack the economic and cultural resources for contesting administrative decisions and weathering temporary or permanent financial shocks (Eubanks 2018; Lageson 2020; Madden et al. 2017). These studies suggest that inaccurate data can threaten individuals' financial security, including in ways that compound existing disadvantage.

Economic insecurity has both material and subjective dimensions. Researchers have focused more heavily on the former, objective changes to economic status (for a review, see Western et al. 2012). This body of work investigates the extent to which and how unpredictable events precipitate fluctuations in household income or assets. Yet insecurity pertains not only to unexpected material hardship, but also to perceptions of such risk. Individuals may feel heightened anxiety about or vulnerability to unpredictable life events in ways not entirely reducible to their objective economic conditions (Cooper 2014; Fullerton, Dixon, and McCollum 2020). Hacker (2008:20) conceptualizes this subjective dimension as "a psychological response to the possibility of hardship-causing economic loss." He goes on to say that, "The psychology of insecurity is crucial, for it motivates many of our personal and social responses to risk…" Subjective insecurity, that is, shapes how people act in the face of unanticipated events.

While social scientists have devoted considerable attention to insecurity, few studies incorporate both resources and perceptions. Moreover, theories that conceptualize perceptions in psychological terms—as we saw above with Hacker—cannot account for the way social structure informs experiences of insecurity. Cooper (2014), for instance, shows how upper-income families often focus on and ratchet up feelings of insecurity in pursuit of even more financial resources while middle- and lower-income families tend to downplay those feelings, lower their expectations, or rely on faith in God to get through insecure times. Responses to insecurity thereby exacerbated economic inequality. We therefore need a distinctly sociological theory of insecurity that simultaneously accounts for material resources, subjective perceptions, and the role of social structure.

IDENTITY THEFT AND INSECURITY: A TRUST-BASED THEORY

In seeking to bridge work on personal data and economic insecurity, I advance a theory of insecurity that builds on prior work by incorporating the role of mistrust in experiences of precarity. Figure 1 diagrams this theory. In what follows, I elaborate on each of its components with respect to identity theft, focusing especially on trust breaches given their relatively overlooked contribution to insecurity.

[Insert Figure 1 about here]

Unanticipated event. The experience of insecurity begins with an unanticipated event like identity theft. Such adverse events suddenly disrupt the flow of individuals' lives, potentially compromising financially-relevant behaviors, strategies, and perceptions. With identity theft, individuals may go to withdraw funds from the ATM, only to discover a drop in their balances; check their credit reports only to identify an unknown inquiry or account; or receive a letter in the mail notifying them of an adverse legal judgment or rejection for government benefits. As past research shows, these occurrences can generate both material and subjective insecurity.

Material insecurity. Unpredictable events like identity theft can cause tangible fluctuations in individuals' economic resources, making it harder to pay bills, meet basic needs, and so forth. Many identity theft victims experience direct losses, out-of-pocket expenses, or difficulties with debt collection, incorrect credit reports, and rejection for other financial resources (Anderson, Durbin, and Salinger 2008; Harrell 2019). Low-income individuals and people of color in particular also face the delay or denial of government benefits (Greene 2021) and may sustain higher financial losses (Reynolds 2020). While this latter finding may result in part from greater exposure to severe cases (Copes et al. 2010), it may also reflect the difficulty of managing material fluctuations with fewer resources (Western et al. 2012).

Subjective insecurity. Unpredictable events can also generate perceptions of insecurity. While researchers have not studied such perceptions explicitly in the context of identity theft, surveys consistently find that many victims—particularly low-income ones—report strong feelings of anxiety and worry consistent with subjective insecurity (Golladay and Holtfreter 2017; Identity Theft Resource Center 2018; Randa and Reyns 2019; Sharp et al. 2004). As Figure 1 shows, such feelings may result from material insecurity. Tangible hardships like financial losses, unanticipated debts, or delayed public benefits can, particularly for those of low socioeconomic position, leave individuals wondering how they will pay bills, meet basic needs, and so forth.

Trust breach(es). Past research, however, suggests that material hardship is not a necessary condition for subjective insecurity. Rather, this study suggests that perceptions of insecurity also result from trust breaches—challenges to individuals' ability to anticipate the future behaviors of other actors or systems on whom their financial lives depend. Trust enables individuals to reduce the complexity of everyday life by acting "as if the uncertain future actions of others were indeed certain" (Lewis and Weigert 1985:971). Sociologically speaking, trustees—those in whom individuals place trust—exist at the micro, meso, and macro levels of social structure. While not a new insight, most general sociological theories conceptualize trust at one or two of these levels (Lewis and Weigert 1985; Luhmann 1979; Ross et al. 2001; Smith 2010a). Giddens (1990:34), for instance, asserts that trust represents a condition of "confidence in the reliability of a person or system, regarding a given set of outcomes or events." Moreover, many empirical studies opt for an altogether different distinction between "particularized" and "generalized" trust that, while useful, tends to focus attention on situations or dispositions rather than levels of social structure (for a review, see Schilke et al. 2021). In contrast, I conceptualize individual trust as operating at the micro, meso, *and* macro levels. Echoing Giddens (1990), I define *interpersonal*, *organizational*, and *systemic trust* as conditions of confidence on the part of individuals in the reliability of other (a) people, (b) organizations, and (c) systems on which they depend.

Crucially, the maintenance of trust cannot be taken for granted (Lewis and Weigert 1985). Unanticipated events expose individuals to contingent futures previously bracketed out by trust in other actors or systems (Ross and Squires 2011), potentially violating that trust. To use our present case, the misuse of an individual's personal data may lead her to mistrust other people—at least one of whom has already exploited her data for personal gain. At the same time, organizations like banks may appear negligent, uncaring, or motivated by financial self-interest. Finally, the individual may lose faith in the security and predictability of systems of identification or associated digital infrastructures like the Internet that apparently failed her or exposed her to risk. My theory accounts for the analytically distinct, though not mutually exclusive, roles of these three types of mistrust in shaping individuals' perceptions of their financial (in)security.

As the examples above suggest, it is not clear how victims will understand the causes of or assign responsibility for unanticipated events like identity theft. By distinguishing between interpersonal, organizational, and systemic trust, we see that they may ultimately lose confidence in one or more actors or systems. How individuals interpret such events therefore shapes (mis)trust and (in)security.

Existing literature on trust breaches and repair acknowledges the importance of this process of "attribution" for shaping the meaning of events and trustors' responses to them (Bies and Tripp 1996; Robinson, Dirks, and Ozcelik 2004). For example, Kim and colleagues (2009:408) assert that, "Given that a trust violation is based on the premise that a trustee has committed some form of transgression, perhaps the most comprehensive way in which trust can be repaired is by affecting the extent to which this premise is ultimately deemed to be true." That is, trustees can impact trustors' attributions in part because there is often (if not always) at least some ambiguity about guilt (also see Bachmann, Gillespie, and Priem 2015; Gillespie and Dietz 2009; Kim et al. 2004).

Despite this (often subtle) recognition of ambiguity, literature on trust breaches and repair faces two related limitations.[2] First, that literature disproportionately focuses on *dyadic* relationships—whether between two individuals, two teams or organizations, or a mix (see Brodt and Neville 2013; Dirks and de Jong 2022:267). Second, it almost exclusively considers ambiguity within a particular relationship identified *a priori* by the researcher. As a result of these limitations, we know relatively little about how individuals interpret unanticipated events that, like identity theft, involve multiple potential trustees—and therefore potential transgressors—at different levels of social structure. Thus, one benefit of utilizing my multi-level conception of individual trust is that it sensitizes researchers to the attributional ambiguity characteristic of unanticipated events in more complex social settings.

Behavioral response. Perceptions of insecurity, as Hacker pointed out, shape how people act in the face of unanticipated events. Perceiving new sources of uncertainty about their financial resources and the behavior of other actors or systems, individuals may engage in practices to stabilize unpredictability or minimize perceived risk (see Author Date). Following trust breaches, these practices are likely to reflect individuals' attributions of blame. In the aftermath of identity theft, interpersonal mistrust may lead individuals to rethink seemingly risky relationships; organizational mistrust may inspire victims to demand greater due diligence from financial institutions; and systemic mistrust may occasion a form of "system avoidance" (Brayne 2014) or advocacy for broader policy changes.

Social position. Finally, social position informs the core components of my theory in various distributional and experiential ways. Figure 1 depicts a few such possibilities, each of which I discuss here. First, individuals are not all equally likely to experience unanticipated hardship. While the qualitative nature of the current study does not enable me to speak to this issue, past studies suggest that higher-income individuals and whites are more likely to experience identity theft but that they also typically experience less severe types of cases (especially misuse of an existing credit card) than low-income people and people of color (Anderson 2006; Copes et al. 2010; Harrell 2019; Reyns 2013; Reyns and Henson 2016).[3]

Second, inequalities can shape how people experience otherwise similar unanticipated events. As mentioned above, financial resources help individuals to weather material fluctuations, thereby minimizing their direct impact on subjective perceptions. Beyond this straightforward sociological insight, my theory also draws attention to how social position may inform experiences of and responses to precarity by shaping sensemaking in terms of trust. Most research posits economic disadvantage and racial marginality as important antecedents of mistrust (Abascal and Baldassarri 2015; Alesina and La Ferrara 2002; Rahn et al. 2009; Smith 2010b; Tyler 2005; but see Simpson et al. 2007). According to this line of work, past and present hardship and neighborhood disorder make low-income people and people of color more likely than whites and higher-income individuals to believe that other people "will exploit or victimize you in pursuit of their goals" (Ross et al. 2001:569). Similarly, their interactions with organizations and institutions are often marked by surveillance, punishment, or neglect—in contrast to organizational responsiveness to or accommodation of more privileged people (Calarco 2018; Lareau 2011; Ray 2019)—thereby contributing to suspicion or resignation (Goffman 2014; Hagan et al. 2018; Sandefur 2007). In sum, sociologists often expect low-income people and people of color to express the greatest levels of mistrust.

Unfortunately, scholars have devoted less attention to how social inequalities inform whether or not and how individuals interpret unpredictable events as breaches of trust. Below, my findings speak to this very issue. While identity theft generated deeper interpersonal mistrust among low-income people and people of color in the study, their economically- and racially-privileged counterparts experienced that event more than others as a breach of trust in organizations they expected to protect them. In shedding light on how social structure shapes interpretations of unpredictable events, these findings complicate accounts uniformly linking disadvantage to mistrust, thereby demonstrating how a multi-level conception of trust can reveal new potential mechanisms for inequality.

DATA AND METHODS

The empirical material for this paper derives from a larger relational qualitative study of identity theft resolution (see Author Date). In that study, I investigated experiences of and efforts to address identity theft through a combination of a) interviews with 45 identity theft victims, b) interviews with 48 organizational personnel—including bank staff, law enforcement personnel, attorneys, and other victim advocates—c) participant observation in financial industry and nonprofit settings, and d) review of documentary sources, such as training materials, industry guides and reports, and legal and regulatory documents.

This paper relies primarily on the interviews with victims of identity theft to elucidate the mechanisms linking experiences and social positions to sensemaking about financial (in)security. That methodology is strongly suited for developing a rich account of identity theft victimization because interviews enable researchers to probe the meanings that individuals ascribe to their experiences (Lamont and Swidler 2014). For the present purposes, interviews offered an ideal means to solicit detailed, process-oriented narratives from individuals regarding how they experienced, interpreted, and ultimately responded to identity theft and its significance for their financial lives.

Recruiting identity theft victims to participate in this study necessitated overcoming their status as a relatively invisible population.[4] I therefore employed a three-pronged approach to recruitment, leveraging 1) online platforms, such as Craigslist, Facebook, and Reddit, 2) referrals from victim assistance organizations, and 3) snowball sampling, and offered a small monetary incentive for participation. Potential participants completed a screening survey to confirm study eligibility and track the demographic composition of the sample.[5] Since the study aimed to interview victims in-person until the onset of the Coronavirus pandemic, the majority of victim interviewees (N = 34) lived or worked in New York City.[6] Beyond geography, I paid particular attention to recruiting individuals with a wide range of backgrounds and experiences (see Table 1). The sample exhibits higher average educational attainment than the general population. Overall, though, its diversity enabled me to identify more general theoretical mechanisms linking identity theft to material hardship and perceptions of insecurity while accounting for intersecting racial and economic inequalities.

[Insert Table 1 about here]

Interviews typically lasted between one and three hours. I asked each interviewee whether they preferred I use their real name or a fictitious name, as well as if they consented to audio recording. Interviewees split over the use of real names but generally consented to audio recording. I recorded and transcribed all such interviews. During all other interviews, I took particularly detailed notes, including striking quotes. Victim interviews focused on three themes: how individuals first discovered and felt about their case ("detection"), the steps they took to address any related issues ("resolution"), and the financial, social, and emotional implications of their experience ("consequences"). Discussion of both trust and economic insecurity came up throughout interviews, but particularly in response to the following question: "How, if at all, has your experience of identity theft affected you?"

The insights derived from victim interviews—particularly the overarching link between identity theft and economic insecurity—were also informed by interviews and participant observation with organizational personnel. All personnel interviewed in the study worked or consulted for organizations that served New Yorkers, though they were situated in cities around the country and generally served national clienteles. I recruited personnel through a mix of 1) networking at professional and industry events, 2) outreach through online professional portals, and 3) snowball sampling. Interviews focused on how they encountered identity theft claims, the steps they and their organizations took to resolve such claims, and the larger issues or challenges they faced during that process. The theme of economic insecurity emerged in these interviews when personnel shared concrete examples of cases as well as in response to the question, "In your work, what do you see as the consequences of identity theft?"

My argument about economic insecurity specifically benefited from over 100 hours I spent shadowing staff from the Identity Theft Resource Center (ITRC), one of the country's leading victim assistance nonprofits dedicated to identity theft. The bulk of my shadowing focused on the organization's call center, which provided Americans around the country with free assistance regarding data breaches and identity theft. There, I sat with call center staff and observed how they counselled callers regarding managing and resolving their particular issues. I also joined staff at events targeting industry and government, where they advocated for greater attention to victims' experiences.

In the call center and at events, staff devoted considerable time to discussing what they referred to as the "aftermath" of identity theft for victims, observations that increased my confidence in the central claims of this article.

I took an abductive approach to analyzing my data (Tavory and Timmermans 2014). I began by searching for surprising findings with respect to existing literature on economic insecurity, using note taking, memoing, and coding processes to facilitate my search. These processes led me to notice that economic insecurity depended not only on material hardship, but also on breaches of trust in other people, organizations, and systems on which victims depended. Moreover, low-income people and people of color seemed to talk about trust breaches more in terms of their social networks.

To systematically evaluate and refine my theory, I returned to the data and re-coded it with respect to the emergent concepts of interest. I operationalized the key concepts as follows. I coded references to actually-occurring fluctuations in income, assets, or other economic opportunities as instances of *material insecurity* and any references to fear or uncertainty about present or future economic wellbeing or opportunities as *perceived insecurity*. I coded any interview segment referring explicitly to mistrust or to a lack of confidence in the behavior of one or more specific or abstract persons as *interpersonal mistrust*, with one exception. Where the mistrusted person or persons appeared to stand in for an organization (i.e., personnel mistrusted as representatives of a company rather than rogue individuals), I coded such references as *organizational mistrust.* That code also included references to suspicion or a lack of confidence in organizations or their units. Finally, references to mistrust of larger systems (e.g., the financial system, the Internet) received the code *systemic mistrust*. To assess variation across these codes, I developed a matrix to visually represent the key codes and attributes. This matrix enabled me to investigate patterns in how race and class related to insecurity, confirming low-income and minority victims' greater interpersonal mistrust, but also revealing the surprising finding linking racial and economic privilege to organizational mistrust. I also used the matrix to identify negative cases, such as individuals who did not report feeling insecure and those whose expressions of mistrust did not fit the broader racial and economic patterns I identified. These cases helped me further refine my theory.

Throughout this process, I engaged in two additional forms of comparison. First, I considered empirical variation in the types of identity theft—ranging from the misuse of an existing credit or debit card to the opening of a new loan account and the filing of a fraudulent tax return. Past research suggests that these different types vary in their severity, with the misuse of an existing credit or debit card tending to impact victims less seriously than other types (Copes et al. 2010; Harrell 2019). That victims of all types expressed insecurity pointed to that experience as a more fundamental consequence of identity theft rather than only severe cases. Second, I triangulated insights across different types of data—victim interviews, organizational interviews, and participant observation—and existing literature to confirm the theoretical validity of the argument.

FINDINGS

I turn now to the experience of identity theft and the insecurity it generally produced. For data presentation and clarity, I focus on 11 cases selected to demonstrate the key themes of the paper across the diverse backgrounds and experiences in the sample (see Table 2; for more details on case selection, see the Appendix). I begin with a detailed account of four individuals—Laura, Arleen, Ricky, and Simone—and the ways in which they made sense of their financial lives in light of their victimization. Their stories illustrate the general relationships between identity theft, trust breaches, and economic insecurity in the study. Building off these detailed accounts, the second section incorporates additional cases to elaborate on the distinct roles of interpersonal, organizational, and systemic trust breaches in producing perceptions of insecurity and associated behavioral responses. I then show how race and class informed individuals' experiences of material hardship, perceptions of trust breaches, and associated responses. Finally, I consider the role of past experiences in moderating insecurity.

[Table 2 about here]

Experiencing Insecurity

Identity theft exposed individuals to unanticipated costs or constraints in a variety of ways. Some victims suddenly sustained losses due to unreimbursed transactions, fees, and other expenses. Others faced surprise debts, which creditors or debt collectors generally reported to credit bureaus, thereby damaging credit scores. On occasion, those

organizations even garnished wages or froze assets to recoup the debt. Finally, identity theft negatively impacted the disbursement of some individuals' government benefits like tax refunds and welfare benefits. These experiences left victims worrying about the stability of their financial lives.

Laura.—A stay-at-home mother of two from the St. Louis metro area, Laura (White [W], Upper-Income [UI]) considered her family the "average suburban family." With her degree in accounting, she managed the family's taxes in addition to performing maintenance tasks around the house and restoring antique furniture for fun. In April 2015, a few weeks before the family closed on a new home, she e-filed their taxes only to receive a rejection email from the IRS notifying her that a return had already been filed. Panicking, she called a longtime friend who worked there. The friend reassured her and told her to assemble her paperwork and visit the local IRS office the next business day. The following day, after a four-hour wait, Laura met with a staff person who looked into her claim and shared with her that someone had made two attempts to file returns under her husband's SSN, both of which got rejected because they claimed an unusually high number of dependents. The staff person then manually entered Laura's return and straightened things out. As a result of the ordeal, the family's tax return got delayed six months, but in Laura's words, "that didn't bother us." "To be honest," she said, "we have always seen that refund as just money to go into the savings account in the bank. It's not money that we count on like so many Americans do."

Even so, Laura found the experience unsettling. She began worrying about her family's personal information and how its exposure could jeopardize them financially. Since she could not identify how the perpetrator obtained her information, she reported increasing her vigilance about her and her children's data, such as "not saying happy birthday to my children on my social media account" (which would publicize their birthdates). Such measures, however, offered little comfort, since she knew that her and her husbands' information had already been compromised and suspected the same might be true of her children. Instead, she held the IRS and other organizations responsible for properly identifying people. "The IRS needs to…get better at ensuring that when we file tax returns, it is in fact ours and not someone else's. …It's not my job to police the tax filings. It's their job to do that, and they're doing a bad job. I didn't trust the government before. I really don't trust them now. Our information is not safe anymore." Laura worried most that her children's credit would be "destroyed" by someone seeking personal financial gain. "So that's my biggest fear, right? Because if we, as a society, can't get loans, can't get credit, then it sort of stifles what…we want to do in our lives." Although the fraudulent tax returns had little material impact, Laura's experience shook her confidence in the IRS specifically and the federal government in general, leaving her feeling that her and her family's data—and with it their financial lives—were vulnerable.

Arleen.—Ohio resident Arleen (Biracial, Low-Income [LI]) was living with her mother and working as a cashier at the grocery store chain Schottenstein. So "carefree," she did not bat an eye when she lost her wallet containing her Social Security card and a copy of her birth certificate. Sometime soon thereafter, she received a phone call from a bank notifying her of the need to pay down the balance on her credit card—something she had never possessed. She still thought nothing of it, attributing it to an issue involving someone else with the same name. Then the police showed up at her workplace and arrested her for writing bad checks. "Needless to say, I lost the job behind it."

Arleen was soon released on recognizance (i.e., without bail), but spent the following months in and out of court. She was finally exonerated after a handwriting expert determined that her handwriting sample did not match the signature on the checks. Still, the experience marked her with a criminal record that required explanation. Anytime she applied for a job or an apartment, Arleen felt compelled to warn the employer or landlord about the charge and implore them—however fruitlessly—to consider the disposition.[7] As a result of her experience, she questioned the poor due diligence of financial institutions that made people like her vulnerable. "Evidently, somebody took a fake ID and they didn't notice this was a fake ID?" Arleen also expressed concern regarding the company she kept. Having her identity stolen made her suspicious of the people in her life, especially when inviting them into her home:

> Arleen: I only have one or two people that are close to me that know that type of information. Stuff like that affects the…you think about people that you bring in your house. You know. You know.
>
> [Author]: [*pause*] How does it affect how you think about which people to bring into your house?

> Arleen: To be honest, I don't keep too much company in my house. … You just can't trust everybody you meet. Even people you've had around you for a while can be shiesty.[8] [I'm] not as open to talk to new people because you never know what their agenda is.

Seeing more clearly the vulnerability of personal data, Arleen purported distancing herself from the people around her to limit her risk.

Ricky.—A serial tech entrepreneur, Ricky (W, MI) spent his days working on as-yet unprofitable side "ventures," volunteering as a first responder, and caring for his daughter and twin young autistic sons. Before getting married and having children, his life in the early aughts seemed to him like "living the dream" complete with "limited-edition" luxury vehicles and a vibrant dating life. Then, in 2005, his friend and business partner suddenly ran off with a secretary at their company, formed a new business, and used Ricky's personal information to access credit lines for hundreds of thousands of dollars. Ricky felt "destroyed." He first contacted the banks, who he said rejected his disputes, and then a handful of attorneys, who demanded retainers while promising dubious benefits. Frustrated and without recourse, he resigned himself to financial ruin and a long slow path to recovery.

Fast forward to 2018. Ricky wrote a check that bounced and, after looking into his accounts, realized his bank was withdrawing $1,000 a month from his account to pay off a debt he knew nothing about. He soon discovered that a longtime friend and employee in one of Ricky's new ventures had used his personal information to take out $10,000 in loans, lines of credit, and cash from one of Ricky's accounts. Considering his past experience, Ricky "jumped into action the moment that I found out." Although the banks eventually approved Ricky's dispute, he lost "a couple of thousand dollars" of the cash taken from his account, which he had failed to report within the legally-mandated timeframe.[9]

According to Ricky, the two episodes led him to question whether banks cared about him. In his impression, their financial interest in avoiding fraud losses outweighed his needs as a victim. "My bank's attitude is, 'Oh wow, if this guy reports identity theft, we may have to give him money back from our slush fund,' if you will. Banks fight to prevent you from getting money." Banks were not the only financial institutions on whom Ricky cast suspicion; he had serious doubts about debt collectors as well. Theirs was a "dirty business" in which the companies would "do whatever they need to do to collect money." As a result, Ricky lived in a degree of perpetual fear about debt collectors coming for him, even avoiding traditional wages that they could detect and garnish. He also worried about authentication processes, which now relied on compromised information of his that could not be recovered:

> Somebody got my Social Security Number, my date of birth, my mother's maiden name. They know the make and model of my first car. Well, all the questions that they ask you on a credit card application. … I mean, there's people that know this information about me … and at any point in life they can still apply for credit, maybe get it using my credentials. That's scary.

Ricky expressed alarm that credit card applications relied on information of his that was no longer private. Notice also how he referred to the perpetrators—both of whom were close business associates—in impersonal terms ("somebody," "they," "there's people"). These points reinforce how when it came to his financial future, Ricky principally worried about organizations and systems like banks, debt collectors, and authentication processes which he no longer believed would—or even could—protect his interests.

The cases of Laura, Arleen, and Ricky illustrate how financial insecurity can accompany very different material shocks associated with personal data. Yet as the following account of Simone's experience demonstrates, identity theft can generate perceptions of insecurity even without impacting individuals' resources.

Simone.—Originally from California, Simone's (W, LI) pursuit of a college degree had taken many twists and turns. In 2011, after securing public assistance and her own apartment in New York City, she enrolled in one of the city's public colleges to finally complete her degree. The following year, while checking her credit report, she noticed that someone in Michigan had attempted to obtain a car loan in her name and been denied by the bank—an outcome Simone attributed to her already bad credit. The experience, she said, "freaked me out." According to her, she Googled what to do and then called the Federal Trade Commission (FTC) hotline. When she explained that she had no idea how her information got out, the staff person told her that identity theft often happens at colleges because of their use of SSNs.

Simone had already been in what she described as a questionable and abusive romantic relationship with one of the college's administrators, so the new information made her feel more "sketchy" and "unsafe" there. She began worrying about the school's hiring procedures and regular requests for SSNs. "It's not really safe because apparently your Social Security Number, it's attached to a lot of things. For me, I have food stamps and Medicaid, so it's attached to all that, not just whether I go to school or not." Simone's experience also shook her confidence in the whole of digital life that depended on data exchange. She referenced an article in New York Magazine about how "we're living in the Matrix." "It's kind of like that, you know what I'm saying? You know that you're not going to put your wallet [down] so that somebody can steal your wallet. But with identity theft, it's very different. It's not this physical reality that you're experiencing." In an increasingly virtual world, she sensed that the rules of the game had changed, leaving her wondering how to protect herself financially. Although identity theft did not tangibly impact Simone's financial resources, it diminished her trust in her college and the Internet—both of which appeared to hold some sway over her financial wellbeing—leaving her feeling more insecure.

Trust Breaches and the Production of Subjective Insecurity

While material hardship can generate perceived insecurity, it is not a necessary nor typically sufficient condition for those feelings. Trust breaches play a crucial role. As each of the cases above showed, identity theft often threatens individuals' ability to anticipate the behavior of other people, organizations, or systems on which they depend, making their financial lives appear more precarious. In what follows, I build on these initial accounts, incorporating additional cases to elaborate on how identity theft can compromise each of the three forms of trust—interpersonal, organizational, and systemic—leading to perceived insecurity. These forms of mistrust should not be seen as mutually exclusive; many individuals experienced multiple, or even all three. Yet as I discuss further below, race and class shaped the kinds of mistrust individuals expressed and their strategies for managing it.

Interpersonal.—For some individuals, identity theft undermined their trust in the people around them, including even friends and family. Suddenly, personal data seemed like a conscious vulnerability that others might exploit to "take advantage." As Arleen put it, "Even people you've had around you for a while can be shiesty." She was not alone in feeling this.

In 2018, after escaping an abusive boyfriend in New Jersey, Warren (B, LI) moved to New York City in search of his own place and a better life. While apartment hunting, however, he began receiving rejection letters and calls from landlords apparently due to his credit. Later, while attempting to get an iPad through a promotional deal at a local phone company, he learned the details: He supposedly owed a cable provider in Newark, NJ $1,500 for a past-due account associated with an address where he said his cousin lived with her boyfriend. The situation left Warren feeling vulnerable and mistrustful of those around him, any of whom might "take advantage." "[People] don't care about your feelings. Your wellbeing—they don't care. All they care about is what they can get from it." From that moment on, he resolved never to "make dumb mistakes, like make that mistake again":

> You don't have nobody come stay with you. You don't move out your place and go stay with no friends and no family. No, none of that. You don't go say, "Oh, can you go to my house and check my mail?" Like, no. Because you don't know. … We live in a world of, you can have fun, you can have friends, but you don't give nobody your information and you don't let nobody stay in your place. I understand that. And I had to go through this to see you don't need a man. You don't need no family members coming to see you and check on you. Take care of yourself.

Warren never once complained to me about the cable company. When it came to organizations, he said, "I don't have no personal bad issues with them. …I don't see nothing wrong." He had confidence in institutional trust mechanisms like professional ethical codes and employment documents ("they sign stuff that they won't steal my information and use it for any other things"). Instead, he understood his experience of identity theft primarily in terms of interpersonal risk, which also shaped his response. Fearing those around him, he reinterpreted his former offering of and reliance on informal assistance—though not directly tied to his cousin—as a source of vulnerability to assiduously avoid.

Based on Warren's experience, mistrust in one's social network might appear to result from attributing (rightly or wrongly) one's victimization to someone close. While such personal experience likely plays some role, it cannot

explain why individuals like Ricky—whose story above involved significant hardship at the hands of two business associates and friends—downplayed such mistrust. Nor can it account for interpersonal mistrust in cases where individuals reported victimization at the hands of a faceless stranger. Tina (B, LI) received a letter from the IRS one day notifying her that she owed $20,000 in back taxes. After claiming identity theft at the IRS office, she learned in later correspondence that the perpetrator lived nearly a thousand miles away in Georgia. Fearing that it would happen again, however, she reported implementing strategies to protect herself, including not only monitoring her accounts daily, but also leaving her old social circle comprised of mostly "rowdy, street people … because I felt like maybe one of them could have done it." Her new circle included "better black people," people who are "working and they're doing constructi[ve] things," people she felt she could trust not to steal her personal information. "It's much better. I don't have to worry." Interpersonal mistrust can arise even in cases with no apparent personal connection.

Organizational.—Unlike Warren, who expressed relative faith in organizations, many individuals experienced identity theft as a betrayal of organizational trust. Laura lost confidence in the IRS and other businesses to implement proper data protections and authentication procedures. Arleen questioned financial institutions' due diligence. Ricky worried about banks honoring his disputes and debt collectors garnishing his wages. Such individuals blamed organizations at least partly for their victimization. In turn, identity theft left them feeling as if their financial lives hung in the balance, at the mercy of opaque, insufficient, or self-interested organizational practices.

Jamie (W, MI) worked as an investment analyst in the advertising industry and loved playing softball on weekends. When she discovered nearly $2,000 in combined fraudulent charges on her Bank of America debit card and Macy's store card, she felt like she was in a "nightmare." Following those experiences, Jamie lost faith in the ability of Bank of America and Macy's to secure her information. "You're this multi-billion-dollar company and you can't prevent this? … I think it made me wary of keeping my accounts open with them, because I don't know if I can really trust you. How are you going to prevent this from happening again?" The betrayal of trust suddenly made her feel financially vulnerable. "I'm giving them my money to hold. I'm not trusting you with my life, but if my money is gone, I can't pay my bills. I can't eat. I can't do anything. It's scary." Despite her misgivings, however, she maintained both accounts, concerned that closing them would reflect badly on her as a consumer. Still, she instituted alerts to personally monitor her accounts and opened a new account at a different bank to test the waters.

Like Jamie, many individuals blamed organizations for failing to protect them. Since those organizations played a crucial role in individuals' current financial situations, however, this loss of confidence provoked considerable insecurity regarding their financial wellbeing and aspirations. As a result, some switched banks or forswore certain financial tools. At the very least, most articulated claims for organizational practices that would better protect them. Chuck's (W, UI) account of identity theft illustrates this response to insecurity. Around five years before we met, he went to his local Citibank to use the ATM and noticed that $7,000 had been withdrawn from his account. He felt like he had been "held up." The bank supposedly looked into the incident, identified that a check had been written by unknown individual, and then refunded his money, but six months later that exact scenario happened again. Although the bank closed his account and opened a new one for him after the second incident, Chuck expressed frustration regarding the bank's apparent willingness to tolerate identity theft, putting himself and others at risk:

> Chuck: Now what did frustrate me a bit is that the bank was just going, "We're going to close out your account and start you from scratch as if you never had anything here." But they didn't really want to do any internal investigations and see what was going on. …I felt that this is happening to me, it could be happening to other people too. And it could possibly happen [to me] again. …I was glad they did back up and they did give me all the funds back, but it was still frustrating that they didn't want to go into it more.
>
> [Author]: What do you wish they would have done?
>
> Chuck: Possibly gone through records to see what checks were written, that they took the funds out of the account. See whose account that [check] was written from and then go after them and see what's happening. Because [the bank employee] did tell me that they did find a check. But they didn't sort of really investigate who wrote the check and do any other things.

Based on his interactions with bank employees, Chuck believed that his bank had conducted only cursory investigations and did not pursue the perpetrators following his two incidents. This observation—whether accurate or not[10]—left him feeling vulnerable to future losses. In response, he articulated a desire to see the organization do more to protect him and other customers.

Systemic.—Finally, identity theft not only shook confidence in other people and organizations, but also in broader sociotechnical systems associated with the American economy. For many victims, their experiences highlighted how institutionalized procedures necessitating the regular exchange of personal data exposed it to potential misappropriation. As with Simone, some victims also felt uncertain about the digital infrastructures on which data so often circulated. Making matters worse, they sometimes recognized that personal data could not be retrieved nor in many cases (particularly SSNs) easily changed.

In 2013, Lucia (W, UI) was working as an economist and living in Los Angeles with her husband and dogs when, out seeing a film one night, someone stole her wallet. She reported the theft to the police and her bank, Wells Fargo, the very next day. Four months later, however, someone began using the supposedly cancelled debit card, eventually racking up nearly $100,000 in transactions and cash advances despite a card limit of only $2,500.[11] The experience led her not only to mistrust Wells Fargo, with whom she ceased banking, but also the "system" of personal information relying on the SSN:

> The reality is that I think our system is completely inadequate in how our personal information is basically readily available. The fact that we use the Social Security Number for all these things and it's a number that anybody can basically figure out on you. It's such an inadequate system, especially today. And I think something needs to be done about it. It's just not possible to continue this way. … With hacking of Equifax and other services, people's information … is out there for basically anybody to see and this is all you need to open an account or get a mortgage, get financing or credit or whatever in somebody's name. This is crazy.

Lucia's awareness of the American financial system's dependence on SSNs generated fears about the security of her financial future. In response, she demanded systemic change. For individuals like Lucia, systems they formerly took for granted or believed in suddenly appeared suspect, liable to compromise their financial wellbeing.

The preceding accounts demonstrate how subjective insecurity emerges through three distinct pathways associated with interpersonal, organizational, and systemic trust. That is, individuals feel financially insecure in part because they struggle to anticipate how other people, organizations, and systems will operate. As the following section shows, distinguishing between these three forms of mistrust also helps untangle the complex ways that social inequality informs insecurity.

Race, Class, and Insecurity

Implicit thus far, experiences of identity theft and the financial perceptions they engender are informed by individuals' positions within unequal social systems. Specifically, race and class shape how identity theft impacts material wellbeing, trust, and responses to insecurity.

First, consistent with sociological expectations, economic resources helped people avoid or cope with material hardship resulting from identity theft. Individuals like Laura (W, UI) had surplus financial resources they could draw on to pay bills, resolve outstanding obligations, and even advocate for themselves, including by hiring a private attorney to assist with disputes (also see Author Date). As a result, perceived insecurity among the economically privileged tended to revolve around status attainment, especially purchasing a new home.

In contrast, low-income individuals worried more about paying bills and maintaining steady employment and housing. Material fluctuations like frozen bank accounts or garnished wages squeezed already constrained individuals (also see Greene 2021). As Amy, a legal aid attorney who encountered such issues regularly, put it, "When you're a low-income person, you are living paycheck to paycheck or benefit check to benefit check. And when you can't access those funds, it's just terrifying." Similar stories played out with delayed tax returns. Unlike Laura's family, who put all of their refund into savings, many low-income people depend on the Earned Income Tax Credit (EITC) for debt relief, consumption, and dignity (Sykes et al. 2015). Losing or even waiting for it could cause

significant hardship. Class fundamentally shaped the experience of material fluctuations and associated perceptions of insecurity following identity theft.

Racial and economic positions also informed how identity theft impacted trust (see Table 3). Consistent with past research on mistrust (e.g., Ross et al. 2001; Smith 2010a), low-income individuals and people of color like Arleen, Warren, and Tina expressed suspicion toward their personal networks more than others in the study. While others sometimes worried about strangers, low-income people of color feared revictimization at the hands of family, friends, or acquaintances, who now appeared capable of "taking advantage" in a new way.

[Table 3 about here]

A simple account linking racial and economic disadvantage to mistrust and insecurity, however, fails to account for an important dynamic in the study: organizational mistrust actually emerged more often among more racially and economically privileged individuals in the study. Chuck felt insecure due to a perceived lack of adequate safeguards and investigations at his bank. Laura mistrusted the IRS due to her sense that they were "doing a bad job" monitoring tax filings, but her lack of confidence extended to other organizations that requested her personal information with what she perceived as questionable motivations and inadequate security:

> I have to give my Social Security Number to the doctor's office for crying out loud. So when we fill out new patient forms when you go to the doctor's office, I intentionally don't put our Social Security Numbers on them. …I don't know what they do with that paper. Does it go in a file cabinet somewhere? Do they shred it? They don't protect it. In St. Louis, if you go to a rescue to adopt a dog, you have to put your driver's license number down on the application. Why does an animal rescue need my driver's license number? I'm not giving you that.

After experiencing identity theft, Laura became wary of any organization—financial, medical, veterinary—that requested personal information without both a clear need and evidence of good security practices. She also felt comfortable withholding information from them for her own protection. Intersecting racial and economic positions thus informed insecurity through distinct pathways of mistrust. Unlike their low-income and minority counterparts, middle- and upper-income individuals and whites did not primarily interpret identity theft in interpersonal terms. Rather, they experienced it as an organizational failure.

Race and class differences in mistrust help to explain a final way that social inequalities inform insecurity: coping strategies. In response to identity theft, nearly everyone in the study reported taking measures to protect their data, including monitoring accounts more regularly or shredding personal information (see Author Date). Beyond that, people took different approaches. As Arleen, Tina, and Warren showed, low-income individuals and people of color tended to report responding to their mistrust of others by severing relationships and channels of informal support. In contrast, middle- and upper-income individuals and whites reacted to the perceived breach of organizational trust by articulating demands for greater protection. Some, like Laura, felt entitled to negotiate information sharing with organizations they deemed untrustworthy. Others called or wrote formal letters to companies, government agencies, and public officials to advocate for themselves. Unlike in Cooper's (2014) research, then, privileged individuals were not alone in acting on insecurity; virtually everyone reported taking some practical steps to minimize their exposure to risk. Yet as Cooper found—and I discuss further below—coping strategies and the perceptions on which they are based still potentially reproduce inequality.

Finally, race and class may intersect in shaping mistrust and insecurity. I opted not to employ intersectional language throughout the article since the intersectional categories in this qualitative study are necessarily small. Yet many of my examples above come from low-income people of color and upper-income whites, who articulated the relationships between identity theft and insecurity most clearly. Table 3 further supports this possibility: Low-income people of color both expressed interpersonal mistrust more than other forms of mistrust and more than any other subgroup in the sample, while the same held true with upper-income whites and organizational mistrust. Considered together, these tendencies suggest that inequalities associated with race and class intersect in shaping mistrust and insecurity following identity theft.

Feeling Secure: The Role of Positive Past Experiences

For most individuals in the study, identity theft breached their trust in other people, organizations, or systems on which their financial lives seemed to depend, leaving them feeling insecure.[12] Yet a minority expressed little to no such insecurity. Why did identity theft not affect how they perceived their financial lives? Scholars have identified various factors (e.g., maintaining cognitive consistency [Robinson et al. 2004]) shaping whether individuals interpret events as trust breaches. While numerous factors may prove useful in modeling insecurity, these exceptional cases draw attention to the relevance of one in particular: past experiences.

Stefanie (L, MI) lived with her roommate and longtime friend in a trendy Brooklyn neighborhood and worked nearby in public relations. In February 2020, she received four letters in the mail from Discover. Two contained details about newly-opened checking accounts—one ominously "payable on death" to a name she did not recognize—while the others specified overdrafts on both accounts for $250 and $500 respectively. At work one day, she retreated to the back of her office and called Discover and two credit reporting agencies. After a few weeks, additional letters, and more calls, Stefanie felt satisfied that her case had been resolved. She shared that while the experience had been a "time suck," it had not inspired concern about her financial life.

> I guess I am really trusting of banks and all the experiences that I've had in the past were resolved pretty quickly. So I almost feel disconnected from it in a way because I'm just like, "Oh, it'll get resolved." … And from past experiences, I've never been responsible for charges that were made on my cards that aren't me. I already went into it knowing I'm not going to have any financial burden or responsibility. So that definitely helps going into it.

What differentiated individuals like Stefanie from most victims appeared to be their ability to draw on positive past experiences—what scholars call a "shadow of the past" (Schilke et al. 2021:6). Those experiences—particularly ones involving the successful resolution of fraud claims—helped sustain trust and downgrade perceptions of risk following identity theft. Things had worked out before, so they continued trusting those around them, the organizations in their lives, and the system at large to look out for their interests. In contrast, most individuals in the study interpreted identity theft as a breach of trust that past experiences reinforced (as with Ricky) or at least did not contradict. As a result, they now worried about the security of their financial lives.

DISCUSSION

This article demonstrated how identity theft operates as an important but overlooked source of economic insecurity. Growing organizational reliance on personal data not only increases the value of that data as a form of individual and organizational capital (Fourcade and Healy 2017), but also the opportunities and incentives for others to acquire and abuse it (Hoofnagle 2009, Solove 2002). When such incidents occur—as they do for tens of millions of Americans each year—contemporary approaches to data governance shift many of the associated costs onto individuals (Monahan 2010). Personal data thus becomes a potent source of economic insecurity.

In demonstrating this point, I advanced a novel trust-based theory of economic insecurity. According to that theory, unanticipated events make individuals feel insecure not only by impacting their material resources, but also by shaking their trust in other individuals, organizations, and systems on which their financial lives depend. In turn, these distinct trust breaches inform different behavioral responses to insecurity.

Crucially, social structure shapes how individuals interpret and respond to unpredictable events. Low-income people and people of color like Arleen, Warren, and Tina worried most that personal data offered family, friends, or acquaintances a previously unforeseen way to "take advantage." Facing such fears, they reported severing ties and foreswearing informal assistance. Such interpersonal mistrust is hardly new. Urban ethnographers and survey researchers have long noted how neighborhood disadvantage contributes to feelings of mistrust in low-income communities and communities of color (Desmond 2012a; Hartigan 1999; Rainwater 2006; Ross et al. 2001; Smith 2010a). Making matters worse, public institutions sometimes appropriate social ties in those communities for criminal justice and welfare surveillance (Goffman 2014; Headworth 2019).

What is new here, then, is an account of one implication of the information age for mistrust in disadvantaged communities. Existing theories tend to emphasize how neighborhood characteristics and personal interactions—witnessing neighborhood disorder, not reciprocating or receiving informal assistance, burning and being burned by recent acquaintances—contribute to mistrust. Personal data, however, links individuals to each other and to

organizations over large swaths of space and time. Moreover, if someone "takes advantage," individuals can lose not only their cash or possessions, but also future income (through garnishment) as well as access to housing, utilities, employment, and public benefits (Greene 2021). Theories of trust and urban poverty need to account for these unique—and uniquely severe—risks associated with personal data.

Unlike the experiences of low-income people and people of color, middle- and upper-income individuals and whites like Laura and Chuck primarily interpreted identity theft as a breach of organizational trust. This finding conflicts with the tendency in most research to associate racial and economic privilege with greater trust (Abascal and Baldassarri 2015; Ross, Mirowsky, and Pribesh 2001; Smith 2010b; but see Simpson, McGrimmon, and Irwin 2007). Moreover, sociologists emphasize how organizations generally serve—or bend to the needs of—middle- and upper-income people and whites (Calarco 2018; Ray 2019). Even with identity theft, regulations like the Fair Credit Reporting Act mandate organizational dispute processes largely tailored to those populations (Greene 2021). Despite this overarching tendency, organizations cannot be expected to *always* uphold the interests of privileged people; things are bound to go wrong sometimes. My findings suggest that while organizations may work for middle- and upper-income individuals and whites most of the time, unpredictable events like identity theft have the potential to breach the latter's typical confidence in organizations, exposing them to insecurity. Although this study was not designed to investigate when and how organizations "fail" people of privilege, it nevertheless raises that concern as a compelling line of inquiry for future research.

These race and class differences in how individuals allocate blame or suspicion have potentially important implications for inequality and organizational accountability. First, by generating interpersonal mistrust among low-income people and people of color, identity theft may lead the very individuals who most need informal support to cut themselves off from it. A wealth of research shows how low-income people and people of color rely on networks of kin, friends, and even strangers to get by (Desmond 2012a; Domínguez and Watkins 2003; Sarkisian and Gerstel 2004; Stack 1974). After experiencing identity theft, however, these same relationships appeared like vulnerabilities that necessitated severing ties and foreswearing informal assistance. Such accounts may evince costly but rational protective strategies for managing risk in conditions of deprivation (Ross et al. 2001), contributing to a breakdown in channels of mutual connection and support in the communities that most depend on them.

Second, the reported behavioral differences I identified may exacerbate existing inequalities in organizational accountability. As mentioned above, organizations generally serve or accommodate white and upper-income people. Those same people were more likely than others in this study to interpret identity theft as an organizational failure. In response, they articulated claims—sometimes even in the form of formal letters or complaints—for greater support from the businesses and government agencies they believed should serve their interests. If this finding plays out at scale, organizations may become even more responsive to the needs and demands of a narrow, particularly privileged, segment of society.

What are the sources of these race and class differences? Since they emerged as a surprise finding during abductive analysis, this study was not designed to identify their origins. Nevertheless, it offers suggestive evidence for the complex interplay of a number of factors, including knowledge and prior socialization. First, individuals' understanding of information systems may inform their attributions following identity theft. Early in our interview, for instance, Laura told me that her and her family "had anxiety" associated with "the question of, what if it was somebody that we knew [who] had done this?" After posting about the incident on Facebook, however, she began to learn about others in her city with similar issues around the same time, leading her to downplay the possibility that her family knew the perpetrator. "As you move on and you see other people are experiencing the same thing," she said, "Well, they're not all being violated by somebody that they know. … [T]hen you know that it's not personal." Likewise, recall how Simone became suspicious of her college after learning from an FTC employee that identity theft often happened at colleges. Information about data and fraud could change victims' attributions and associated assessments of ongoing risks. To the extent that knowledge about data and information systems tracks disparities in digital competencies (for a review, see Lutz 2019), it may contribute to the race and class differences observed in this study.

Yet knowledge alone cannot explain differences in mistrust. Knowing that a distant stranger stole her identity did not prevent Tina from feeling that her social circle was capable of such acts. And Ricky harbored no apparent suspicion toward his network despite incontrovertible evidence that both his cases implicated close associates. Other factors beyond knowledge must also come into play, perhaps including enduring differences in socialization. As

recent sociological work shows (Calarco 2018; Lareau 2011; Ray 2019), more privileged people learn from an early age to approach organizations directly with a sense of entitlement, while their more disadvantaged counterparts learn deference in similar situations. In this study, Laura felt confident withholding her personal information from organizations, including doctors, unafraid of losing access to benefits and services. In contrast, Warren spoke about organizational mishandling of personal data as beyond his control ("That you just got to pray on. That, you can't control that") and Tina told me that she was "scared" when she went to the IRS to resolve her case because she "never had contact with … these types of professional people" and felt that when it came to seeking remedy from them, she "couldn't have no power over it." Middle- and upper-income people and whites, therefore, not only expect more from organizations when things go wrong, but also possess dispositions to confront them. Although speculative, these insights about the sources of race and class differences in mistrust highlight a fruitful avenue for future research on inequality in the information age.

Overall, race and class differences in mistrust and their potential links to inequality highlight the importance of the multi-level approach to trust advanced in this article. Sociological theories of trust (Giddens 1990; Lewis and Weigert 1985; Luhmann 1979; Ross et al. 2001; Smith 2010a) rarely account for trustees at the micro, meso, *and* macro levels, while empirical research often chooses the altogether different distinction between "particularized" and "generalized" trust (Schilke et al. 2021; Smith 2010b). Yet racial and economic differences in how people experienced identity theft only became visible by disentangling individuals' (mis)trust in other people, organizations, and systems. My multi-level approach to trust may therefore reveal previously overlooked social differences in trust and their links to inequality.

My findings have a number of additional implications for scholars of trust. First, they draw attention to the complex attributional ambiguity characteristic of unanticipated events like identity theft. By focusing on dyadic relationships predetermined by the analyst, existing research on trust breaches and repair tends to bracket out the necessity for trustors to assign responsibility to some combination of actors or systems potentially implicated in an event. As victims in this study demonstrated, identity theft can raise questions about one's social network, organizational ties, and wider economic, political, and technical systems. Thus, an important task facing researchers of trust breaches is to explore how individuals assign blame and ongoing risk among the various potentially relevant actors or systems.

Second, my findings suggest a fruitful avenue for research on the spillover effects of trust breaches.[13] Past research has identified one such effect, namely that negative events can breach trust in a particular trustee not only for those directly harmed by the event, but also other trustors aware of the incident (Kim et al. 2004, 2009). The present study suggests an additional potential spillover: negative events may breach trust in trustees not directly implicated in the incident but seen to be related in some meaningful way. For Arleen, Tina, and Warren, identity theft shook trust not only in the perpetrator—who Warren knew personally, but Arleen and Tina did not—but also in other family, friends, and acquaintances who they believed were capable of similar harm. Likewise, some victims lost trust not just in a particular organization, but in whole categories of organizations that they believed exposed them to risk, such as community banks and credit unions (for seemingly having insufficient resources to prevent fraud), global banks (for not caring enough about individual customers), and even—in Laura's case—all manner of organizations perceived as collecting personal data with inadequate justification and security. To fully understand the impact of unanticipated events on trust, scholars therefore need to consider not only ostensibly peripheral or unrelated trustors, but also analogous trustees.

The relationships in this article between identity theft, trust, and insecurity merit quantitative testing. In particular, my argument about race and class differences hinged on necessarily small numbers of respondents and grouped together racial minorities in ways that may obscure unique experiences of identity theft. Future research could harness survey and experimental methods to test my general theory along with the potentially intersecting role of race and class. At the same time, my theory of insecurity generalized across other potential factors of interest to sociologists of trust and insecurity. Individuals exist within particular social, organizational, and institutional contexts, including friendship networks, neighborhoods, formal organizations, and legal and policy regimes, each of which have the potential to modify how individuals experience unanticipated events. For example, do certain characteristics of one's social network increase the likelihood one will experience interpersonal mistrust? Future research could further develop my theory by specifying the role of these conditions in shaping (in)security.

Finally, while I focused on a case of financial fraud, my findings arguably speak to the broader consequences of breakdown in information systems, beyond both finances and fraud. First, insecurity may result from data sources

not normally perceived as financial. Function creep and the increasing integration of big data surveillance systems (Brayne 2017) link ostensibly nonfinancial data to financial outcomes and facilitate "error propogation" (Rona-Tas 2017). In the case of consumer credit, for instance, industry professionals and advocates often point to so-called "alternative data," such as utility bills and social media posts, as a solution to credit exclusion for those with no or poor credit histories (Aitken 2017; Kear 2017). Social media data, online reputations, and digital criminal records also play an increasingly critical role in hiring decisions and can precipitate job loss (Draper 2019; Lageson 2020). To the extent such applications achieve widespread adoption, they expand the pool of data on which individuals' financial lives depend. Any breakdowns in the associated information systems are therefore likely to generate economic insecurity.

Second, information breakdowns other than fraud can generate economic insecurity. Like identity theft, transpositional and administrative errors undermine data integrity and expose individuals to economic hardship (Eubanks 2018; Lageson 2020; Wu et al. 2019). Such issues may have very different implications for trust—we should, for instance, expect them to impact interpersonal mistrust less. Yet when the causes of data inaccuracy remain opaque to organizational outsiders—as they often do—individuals affected by administrative data issues may wonder if fraud has taken place.

These possibilities highlight the need for sociologists in a wide range of subdisciplines to attend to breakdowns in information systems. Studies have begun to shed light on how those adverse events impact organizational decision-making and individual wellbeing in such varied settings as finance, healthcare, criminal justice, the labor market, housing, and public benefits (Eubanks 2018; Lageson 2020; Wu et al. 2019). Yet social science research on data-based decision making still primarily focuses on the smooth operation of information systems (Brayne 2017; Fourcade and Healy 2017; Kiviat 2019a; Rosen, Garboden, and Cossyleon 2021). As organizations expand their use of personal data for consequential decisions, research on breakdowns in information systems will prove similarly crucial to understanding contemporary insecurity, inequality, and the links between them.

APPENDIX: CASE SELECTION

I relied on a subset of detailed qualitative cases to demonstrate my theory of how identity theft generates economic insecurity while preserving the complexity of individuals' experiences. My selection of these cases was informed by an analytic table, in which each row corresponded to a respondent and each column to an analytic code. These codes included: race; income; material insecurity; subjective insecurity; interpersonal, organizational, and systemic mistrust; and behavioral responses to insecurity. Ultimately, three principles informed my decision to report on particular cases in my write-up.

First, I selected cases to illustrate the set of broader patterns associated with my theory that I identified across most participants' accounts. For example, I strove to ensure that the small selection of detailed cases included multiple examples of each type of mistrust (interpersonal, organizational, and systemic) as well as multiple people from each social category in my analysis (i.e., white and POC; low-, middle-, and upper-income).

Second, I selected cases that not only illustrated my theory but also offered evidence (individually or jointly with other cases) for why I had rejected alternative explanations of my findings. For example, I chose cases to demonstrate that material losses were not a necessary nor sufficient condition for insecurity, thereby helping support my decision to focus on mistrust. To do so, I sought to maximize the diversity of cases and their material consequences, resulting in the inclusion of cases involving unanticipated credit accounts and loans (Ricky), check fraud (Arleen), tax fraud (Laura, Tina), utilities (Warren), account takeover (Chuck), and charges to existing credit/debit accounts (Jamie, Lucia)—which research tends to depict as less severe (Copes et al. 2010). This range of cases demonstrated the near ubiquity of insecurity, regardless of the types of identity theft individuals experienced (or their social backgrounds). At the same time, that diversity helped demonstrate the weak association in my data between material hardship and perceived insecurity, as I reported on cases ranging from heavy losses (e.g. Ricky) to those with no lasting material consequences (e.g. Simone, Tina). I also selected cases to address the possibility that the race and class differences in mistrust I identified might have resulted from differences in the nature of victimization (e.g. whether the victim personally knew the perpetrator) rather than social background per se. Thus, I included a low-income woman of color who reported interpersonal suspicion despite being victimized by a stranger (Tina) and a middle-income white man who placed greater blame on organizations and systems despite having close personal relationships with the perpetrators of his identity thefts (Ricky). Case selection thereby helped to illustrate the general trends in the study in ways that explained my rejection of alternative interpretations.

Finally, I considered "negative cases" (Tavory and Timmermans 2014) to ensure that I took seriously the full range of experiences among my participants. This decision led me to include the case of someone (Stefanie) who appeared to feel secure following identity theft. Doing so enabled me to illustrate the manner in which I tested and further refined my theory linking identity theft to insecurity through mistrust.

Acknowledgments
Special thanks to Shamus Khan for multiple close readings of and incisive comments on earlier manuscripts. Many thanks as well to Terry Brensinger, Gil Eyal, Marion Fourcade, Michele Gilman, Alondra Nelson, Bonnie Siegler, and Bruce Western for their thoughtful feedback. I am also grateful for having had the opportunity to present versions of this research at Columbia, Princeton, Purdue, Vanderbilt, the University of Wisconsin-Madison, the 2020 Privacy Law Scholars Conference, and the 2020 American Sociological Association Annual Meeting. In addition, I wish to thank the many individuals whose willingness to share their stories made this project possible. The larger project was generously supported by a Doctoral Dissertation Research Improvement Grant from the National Science Foundation (#1921260).

Notes

1. I define personal data as any information that can be used, alone or in conjunction with other information, to identify an individual, or that can be linked to an identified individual. I use the terms "personal data" and "personal information" interchangeably.

2. I am grateful to Oliver Schilke for pointing me in this direction.

3. Differential rates of victimization also appear to relate to the kinds of activities (e.g., online banking and shopping) that individuals engage in (see Reyns 2013; Reyns and Henson 2016), which may intersect with race and class.

4. I was unable to find a single victim support group dedicated to their experience. The discussion forum website Reddit had two user-created pages ("subreddits") devoted to questions about identity theft, which I reviewed and incorporated into my recruitment strategy.

5. The qualitative research protocols used in this article—including the screening survey and interview guide—can be found at https://doi.org/10.7910/DVN/NMHSCJ.

6. The study also included eleven individuals from outside the city, who I interviewed virtually. While I did not design the study to assess the role of geographic context, the major themes in this article did not appear to vary across the two groups.

7. In 2016, Ohio adopted so-called "ban the box" legislation banning public employers from asking about a person's criminal record until after they make a conditional offer of employment. To date, however, no such legislation protects the state's private-sector job-seekers. Moreover, even in states with universal protections, employers may resort to informal practices like Google searches to discover criminal records (Lageson 2020).

8. According to the Urban Dictionary, shiesty—likely derived from shyster—"usually refers to an action that is greedy and/or inconsiderate. When someone is shiesty it means they dont think about others and do things that help them even if they know it harms someone else in anyway." See https://www.urbandictionary.com/define.php?term=Shiesty.

9. The Federal Reserve Board's Regulation E specifies that with credit and debit card fraud "the extent of the consumer's liability is determined solely by the consumer's promptness in notifying the financial institution" (Board of Governors of the Federal Reserve System 2013:12).

10. Bank personnel in this study generally reported withholding information from consumers, supposedly for security reasons. Nevertheless, Chuck's perception that his bank did not go after anyone for the crime aligns with the widely accepted belief even within industry that financial institutions and law enforcement rarely pursue perpetrators.

11. Having never heard of an existing card fraud quite like this, I remained somewhat skeptical until Lucia volunteered slightly-redacted copies of her bank statements from the time that confirmed details of her story.

12. Based on the content and delivery of their accounts, I classified most individuals (34 of 45) in this study as feeling moderately to highly insecure.

13. I am grateful to Oliver Schilke for raising this point.

References

Abascal, Maria, and Delia Baldassarri. 2015. "Love Thy Neighbor? Ethnoracial Diversity and Trust Reexamined." *American Journal of Sociology* 121(3):722–82.

Aitken, Rob. 2017. "'All Data Is Credit Data': Constituting the Unbanked." *Competition & Change* 21(4):274–300.

Alesina, Alberto, and Eliana La Ferrara. 2002. "Who Trusts Others?" *Journal of Public Economics* 85(2):207–34.

Anderson, Keith B. 2006. "Who Are the Victims of Identity Theft? The Effect of Demographics." *Journal of Public Policy & Marketing* 25(2):160–71.

Anderson, Keith B., Erik Durbin, and Michael A. Salinger. 2008. "Identity Theft." *The Journal of Economic Perspectives* 22(2):171–92.

Author. Date.

Author. Date.

Bachmann, Reinhard, Nicole Gillespie, and Richard Priem. 2015. "Repairing Trust in Organizations and Institutions: Toward a Conceptual Framework." *Organization Studies* 36(9):1123–42.

Bies, Robert J., and Thomas M. Tripp. 1996. "Beyond Distrust: 'Getting Even' and the Need for Revenge." in *Trust in Organizations: Frontiers of Theory and Research*, edited by R. Kramer and T. Tyler. 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc.

Board of Governors of the Federal Reserve System. 2013. *Consumer Compliance Handbook: Regulation E: Electronic Fund Transfer Act*. Washington, DC: Board of Governors of the Federal Reserve System.

Bouk, Dan. 2017. "The History and Political Economy of Personal Data over the Last Two Centuries in Three Acts." *OSIRIS* 32:1–22.

Brayne, Sarah. 2014. "Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment." *American Sociological Review* 79(3):367–91.

Brayne, Sarah. 2017. "Big Data Surveillance: The Case of Policing." *American Sociological Review* 82(5):977–1008.

Brensinger, Jordan, and Gil Eyal. 2021. "The Sociology of Personal Identification." *Sociological Theory* 39(4):265–92.

Brodt, Susan E., and Lukas Neville. 2013. "Repairing Trust to Preserve Balance: A Balance-Theoretic Approach to Trust Breach and Repair in Groups." *Negotiation and Conflict Management Research* 6(1):49–65.

Calarco, Jessica McCrory. 2018. *Negotiating Opportunities: How the Middle Class Secures Advantages in School*. New York, NY: Oxford University Press.

Cole, Simon A., and Henry N. Pontell. 2006. "'Don't Be Low Hanging Fruit': Identity Theft as Moral Panic." in *Surveillance and security: technological politics and power in everyday life*, edited by T. Monahan. New York: Routledge.

Cooper, Marianne. 2014. *Cut Adrift: Families in Insecure Times*. Berkeley: University of California Press.

Copes, Heith, Kent R. Kerley, Rodney Huff, and John Kane. 2010. "Differentiating Identity Theft: An Exploratory Study of Victims Using a National Victimization Survey." *Journal of Criminal Justice* 38(5):1045–52.

Desmond, Matthew. 2012a. "Disposable Ties and the Urban Poor." *American Journal of Sociology* 117(5):1295–1335.

Desmond, Matthew. 2012b. "Eviction and the Reproduction of Urban Poverty." *American Journal of Sociology* 118(1):88–133.

Dirks, Kurt T., and Bart de Jong. 2022. "Trust Within the Workplace: A Review of Two Waves of Research and a Glimpse of the Third." *Annual Review of Organizational Psychology and Organizational Behavior* 9(1):247–76.

Domínguez, Silvia, and Celeste Watkins. 2003. "Creating Networks for Survival and Mobility: Social Capital Among African-American and Latin-American Low-Income Mothers." *Social Problems* 50(1):111–35.

Draper, Nora A. 2019. *The Identity Trade: Selling Privacy and Reputation Online*. New York: New York University Press.

Dwyer, Rachel E. 2018. "Credit, Debt, and Inequality." *Annual Review of Sociology* 44(1):237–61.

Eubanks, Virginia. 2018. *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor*. New York: St. Martin's Press.

Fourcade, Marion, and Kieran Healy. 2017. "Seeing like a Market." *Socio-Economic Review* 15(1):9–29.

Fullerton, Andrew S., Jeffrey C. Dixon, and Destinee B. McCollum. 2020. "The Institutionalization of Part-Time Work: Cross-National Differences in the Relationship between Part-Time Work and Perceived Insecurity." *Social Science Research* 87:102402.

Gates, Kelly. 2010. "The Securitization of Financial Identity and the Expansion of the Consumer Credit Industry." *Journal of Communication Inquiry* 34(4):417–31.

Giddens, Anthony. 1990. *The Consequences of Modernity*. Stanford, Calif: Stanford Univ. Press.

Gillespie, Nicole, and Graham Dietz. 2009. "Trust Repair After An Organization-Level Failure." *Academy of Management Review* 34(1):127–45.

Goffman, Alice. 2014. *On the Run: Fugitive Life in an American City*. Chicago, IL: University of Chicago Press.

Golladay, Katelyn, and Kristy Holtfreter. 2017. "The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes." *Victims & Offenders* 12(5):741–60.

Greene, Sara Sternberg. 2021. "Stealing (Identity) From the Poor." *Minnesota Law Review* 106:59–124.

Hacker, Jacob S. 2008. *The Great Risk Shift: The New Economic Insecurity and the Decline of the American Dream*. New York: Oxford University Press.

Hagan, John, Bill McCarthy, Daniel Herda, and Andrea Cann Chandrasekher. 2018. “Dual-Process Theory of Racial Isolation, Legal Cynicism, and Reported Crime.” *Proceedings of the National Academy of Sciences* 115(28):7190–99.

Haggerty, Kevin D., and Richard V. Ericson. 2000. “The Surveillant Assemblage.” *The British Journal of Sociology* 51(4):605–22.

Harrell, Erika. 2019. *Victims of Identity Theft, 2016*. Washington, DC: Bureau of Justice Statistics.

Hartigan, John, Jr. 1999. *Racial Situations: Class Predicaments of Whiteness in Detroit*. Princeton, NJ: Princeton University Press.

Headworth, Spencer. 2019. “Getting to Know You: Welfare Fraud Investigation and the Appropriation of Social Ties.” *American Sociological Review* 84(1):171–96.

Himmelstein, David U., Deborah Thorne, Elizabeth Warren, and Steffie Woolhandler. 2009. “Medical Bankruptcy in the United States, 2007: Results of a National Study.” *The American Journal of Medicine* 122(8):741–46.

Hollister, Matissa. 2011. “Employment Stability in the U.S. Labor Market: Rhetoric versus Reality.” *Annual Review of Sociology* 37(1):305–24.

Hoofnagle, Chris Jay. 2009. “Internalizing Identity Theft.” *UCLA Journal of Law and Technology* 13(2):1-36.

Houle, Jason N., and Danya E. Keene. 2015. “Getting Sick and Falling behind: Health and the Risk of Mortgage Default and Home Foreclosure.” *J Epidemiol Community Health* 69(4):382–87.

Identity Theft Resource Center. 2018. *The Aftermath: The Non-Economic Impacts of Identity Theft, 2018*. San Diego, CA: The Identity Theft Resource Center.

Kalleberg, Arne L. 2018. *Precarious Lives: Job Insecurity and Well-Being in Rich Democracies*. Cambridge, UK Medford, MA: Polity.

Kear, Mark. 2017. “Playing the Credit Score Game: Algorithms, ‘Positive’ Data and the Personification of Financial Objects.” *Economy and Society* 46(3–4):346–68.

Kim, Peter H., Kurt T. Dirks, and Cecily D. Cooper. 2009. “The Repair of Trust: A Dynamic Bilateral Perspective and Multilevel Conceptualization.” *The Academy of Management Review* 34(3):401–22.

Kim, Peter H., Donald L. Ferrin, Cecily D. Cooper, and Kurt T. Dirks. 2004. “Removing the Shadow of Suspicion: The Effects of Apology Versus Denial for Repairing Competence- Versus Integrity-Based Trust Violations.” *Journal of Applied Psychology* 89(1):104–18.

Kirchner, Lauren, and Matthew Goldstein. 2020. “Access Denied: Faulty Automated Background Checks Freeze Out Renters.” *The Markup* and the *New York Times*, May 28.

Kiviat, Barbara. 2019a. “The Art of Deciding with Data: Evidence from How Employers Translate Credit Reports into Hiring Decisions.” *Socio-Economic Review* 17(2):283–309.

Kiviat, Barbara. 2019b. “The Moral Limits of Predictive Practices: The Case of Credit-Based Insurance Scores.” *American Sociological Review* 84(6):1134–58.

Krippner, Greta R. 2012. *Capitalizing on Crisis: The Political Origins of the Rise of Finance*. Cambridge, MA: Harvard University Press.

Krippner, Greta R. 2017. “Democracy of Credit: Ownership and the Politics of Credit Access in Late Twentieth-Century America.” *American Journal of Sociology* 123(1):1–47.

Lageson, Sarah Esther. 2020. *Digital Punishment: Privacy, Stigma, and the Harms of Data-Driven Criminal Justice*. New York: Oxford University Press.

Lamont, Michèle, and Ann Swidler. 2014. "Methodological Pluralism and the Possibilities and Limits of Interviewing." *Qualitative Sociology* 37(2):153–71.

Lareau, Annette. 2011. *Unequal Childhoods: Class, Race, and Family Life*. Univ of California Press.

Lewis, J. David, and Andrew Weigert. 1985. "Trust as a Social Reality." *Social Forces* 63(4):967–85.

Luhmann, Niklas. 1979. *Trust and Power*. London: Polity.

Lutz, Christoph. 2019. "Digital Inequalities in the Age of Artificial Intelligence and Big Data." *Human Behavior and Emerging Technologies* 1(2):141–48.

Madden, Mary, Michele Gilman, Karen Levy, and Alice Marwick. 2017. "Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans." *Washington University Law Review* 95:53–126.

Marron, Donncha. 2008. "'Alter Reality': Governing the Risk of Identity Theft." *The British Journal of Criminology* 48(1):20–38.

Marx, Gary T. 2016. *Windows into the Soul: Surveillance and Society in an Age of High Technology*. Chicago: The University of Chicago Press.

Monahan, Torin. 2010. *Surveillance in the Time of Insecurity*. New Brunswick, N.J: Rutgers University Press.

Pew Research Center. 2019. *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*. Washington, DC: Pew Research Center.

Porter, Theodore M. 1996. *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life*. Princeton, N.J.: Princeton University Press.

Poster, Mark. 1990. *The Mode of Information: Poststructuralism and Social Context*. Chicago: University of Chicago Press.

Rahn, Wendy M., Kwang Suk Yoon, Michael Garet, Steven Lipson, and Katherine Loflin. 2009. "Geographies of Trust." *American Behavioral Scientist* 52(12):1646–63.

Rainwater, Lee. 2006. *Behind Ghetto Walls: Black Families in a Federal Slum*. New Brunswick, NJ: Routledge.

Randa, Ryan, and Bradford W. Reyns. 2019. "The Physical and Emotional Toll of Identity Theft Victimization: A Situational and Demographic Analysis of the National Crime Victimization Survey." *Deviant Behavior* 1–15.

Ray, Victor. 2019. "A Theory of Racialized Organizations." *American Sociological Review* 84(1):26–53.

Reynolds, Dylan. 2020. "The Differential Effects of Identity Theft Victimization: How Demographics Predict Suffering out-of-Pocket Losses." *Security Journal*.

Reyns, Bradford W. 2013. "Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses." *Journal of Research in Crime and Delinquency* 50(2):216–38.

Reyns, Bradford W., and Billy Henson. 2016. "The Thief With a Thousand Faces and the Victim With None: Identifying Determinants for Online Identity Theft Victimization With Routine Activity Theory." *International Journal of Offender Therapy and Comparative Criminology* 60(10):1119–39.

Robinson, Sandra L., Kurt T. Dirks, and Hakan Ozcelik. 2004. “Untangling the Knot of Trust and Betrayal.” in *Trust and Distrust in Organizations: Dilemmas and Approaches*, edited by R. M. Kramer and K. S. Cook. Russell Sage Foundation.

Rona-Tas, Akos. 2017. “The Off-Label Use of Consumer Credit Ratings.” *Historical Social Research* 42(1):52–76.

Rosen, Eva, Philip M. E. Garboden, and Jennifer E. Cossyleon. 2021. “Racial Discrimination in Housing: How Landlords Use Algorithms and Home Visits to Screen Tenants.” *American Sociological Review* 00031224211029618.

Ross, Catherine E., John Mirowsky, and Shana Pribesh. 2001. “Powerlessness and the Amplification of Threat: Neighborhood Disadvantage, Disorder, and Mistrust.” *American Sociological Review* 66(4):568–91.

Ross, Lauren M., and Gregory D. Squires. 2011. “The Personal Costs of Subprime Lending and the Foreclosure Crisis: A Matter of Trust, Insecurity, and Institutional Deception.” *Social Science Quarterly* 92(1):140–63.

Rule, James B. 1973. *Private Lives and Public Surveillance*. London: Allen Lane.

Sandefur, Rebecca L. 2007. “The Importance of Doing Nothing: Everyday Problems and Responses of Inaction.” Pp. 112–32 in *Transforming Lives: Law and Social Process*, edited by P. Pleasence, A. Buck, and N. J. Balmer. Rochester, NY: Social Science Research Network.

Sarkisian, Natalia, and Naomi Gerstel. 2004. “Kin Support among Blacks and Whites: Race and Family Organization.” *American Sociological Review* 69(6):812–37.

Schilke, Oliver, Martin Reimann, and Karen S. Cook. 2021. “Trust in Social Relations.” *Annual Review of Sociology* 47(1):annurev-soc-082120-082850.

Sharp, Tracy, Andrea Shreve-Neiger, William Fremouw, John Kane, and Shawn Hutton. 2004. “Exploring the Psychological and Somatic Impact of Identity Theft.” *Journal of Forensic Sciences* 49(1):1–6.

Simpson, Brent, Tucker McGrimmon, and Kyle Irwin. 2007. “Are Blacks Really Less Trusting than Whites? Revisiting the Race and Trust Question.” *Social Forces* 86(2):525–52.

Smith, Sandra Susan. 2010a. *Lone Pursuit: Distrust and Defensive Individualism Among the Black Poor*. New York: Russell Sage Foundation.

Smith, Sandra Susan. 2010b. “Race and Trust.” *Annual Review of Sociology* 36(1):453–75.

Solove, Daniel J. 2002. “Identity Theft, Privacy, and the Architecture of Vulnerability.” *Hastings Law Journal* 54:1227–76.

Solove, Daniel J. 2012. “Privacy Self-Management and the Consent Dilemma.” *Harvard Law Review* 126(7):1880–1903.

Stack, Carol B. 1974. *All Our Kin: Strategies for Survival in a Black Community*. New York, NY: Basic Books.

Sullivan, Esther. 2018. *Manufactured Insecurity: Mobile Home Parks and Americans’ Tenuous Right to Place*. Oakland, CA: University of California Press.

Sykes, Jennifer, Katrin Križ, Kathryn Edin, and Sarah Halpern-Meekin. 2015. “Dignity and Dreams: What the Earned Income Tax Credit (EITC) Means to Low-Income Families.” *American Sociological Review* 80(2):243–67.

Tavory, Iddo, and Stefan Timmermans. 2014. *Abductive Analysis: Theorizing Qualitative Research*. Illustrated Edition. Chicago: University of Chicago Press.

Tedder, Krista, and John Buzzard. 2020. “2020 Identity Fraud Study: Genesis of the Identity Fraud Crisis.” *Javelin*. Retrieved May 23, 2020 (https://www.javelinstrategy.com/coverage-area/2020-identity-fraud-study-genesis-identity-fraud-crisis).

Tyler, Tom R. 2005. “Policing in Black and White: Ethnic Group Differences in Trust and Confidence in the Police.” *Police Quarterly* 8(3):322–42.

United States Department of Justice. 2017. “Identity Theft - Department of Justice.” *The United States Department of Justice*. Retrieved October 27, 2018 (https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud).

Vieraitis, Lynne M., Heith Copes, Zachary A. Powell, and Ashley Pike. 2015. “A Little Information Goes a Long Way: Expertise and Identity Theft.” *Aggression and Violent Behavior* 20:10–18.

Viljoen, Salomé. 2021. “A Relational Theory of Data Governance.” *The Yale Law Journal* 82.

Western, Bruce, Deirdre Bloome, Benjamin Sosnaud, and Laura Tach. 2012. “Economic Insecurity and Social Stratification.” *Annual Review of Sociology* 38(1):341–59.

Whitson, Jennifer R., and Kevin D. Haggerty. 2008. “Identity Theft and the Care of the Virtual Self.” *Economy and Society* 37(4):572–94.

Wu, Chi Chi, Michael Best, and Sarah Bolling Mancini. 2019. *Automated Injustice Redux: Ten Years after a Key Report, Consumers Are Still Frustrated Trying to Fix Credit Reporting Errors*. Boston, MA: National Consumer Law Center.

Table 1. Victim Demographics at Time of Interview (N = 45)

	N	%
Age		
18 – 30	9	20%
31 – 45	20	44%
46 – 60	11	24%
60 +	5	11%
Gender		
Female	26	58%
Male	17	38%
Genderqueer/other	2	4%
Race (not mutually exclusive)		
Asian	6	13%
Black	10	20%
White	27	60%
Other	4	14%
Latinx	6	13%
Education		
HS diploma or equivalent	4	9%
Some college or Associates	10	22%
4-year Degree	16	36%
Graduate or Professional Degree	15	33%
Household Income		
Less than $15,000	7	16%
$15,000 - $49,999	15	33%
$50,000 - $99,999	15	33%
$100,000 - $149,999	6	13%
$150,000 or more	2	4%

Table 2. Primary Cases

Name	Age	Gender	Race	Education	Household Income
Arleen	43	Female	Biracial[a]	High school	Less than $15,000 (LI)[b]
Chuck	71	Male	White	Graduate degree	$100,000 – $149,999 (UI)
Corey	47	Male	Black	Some college	$50,000 – $74,999 (MI)
Jamie	26	Female	White	4-year college	$50,000 – $74,999 (MI)
Laura	45	Female	White	Graduate degree	$150,000 or more (UI)
Lucia	40	Female	White	Graduate degree	$150,000 or more (UI)
Ricky	43	Male	White	4-year college	$75,000 – $99,999 (MI)
Simone	40	Female	White	4-year college	Less than $15,000 (LI)
Stefanie	32	Female	Latinx	4-year college	$50,000 – $74,999 (MI)
Tina	46	Female	Black	Some college	$15,000 – $34,999 (LI)
Warren	30	Male	Black	High school	Less than $15,000 (LI)

[a]Arleen identified as black and white

[b]Letters associated household income correspond to individuals' assigned income category; LI = Low-Income, MI = Middle-Income, UI = Upper-Income (also see Table 3).

Table 3. Forms of Mistrust, by Household Income and Race

			Mistrust		
		N	Interpersonal (%)	Organizational (%)	Systemic (%)
Household Income	Low ($0 - $34,999)	14	71	50	57
	Middle ($35,000 - $99,999)	23	39	70	43
	Upper ($100,000+)	8	50	63	38
Race	People of Color (POC)	19	58	47	32
	White	26	46	73	58
Income & Race	Low-Income POC	9	78	56	56
	Upper-Income White	6	33	83	50
	All Others	30	43	60	43

Note: The three forms of mistrust are not mutually exclusive. The table reports row percentages for each form. Those percentages emerged from a binary (i.e., present/not present) coding of interview data. While they illustrate the themes in my analysis, that analysis also relied on a deeper consideration of the qualitative emphasis on each form of mistrust in individuals' accounts.

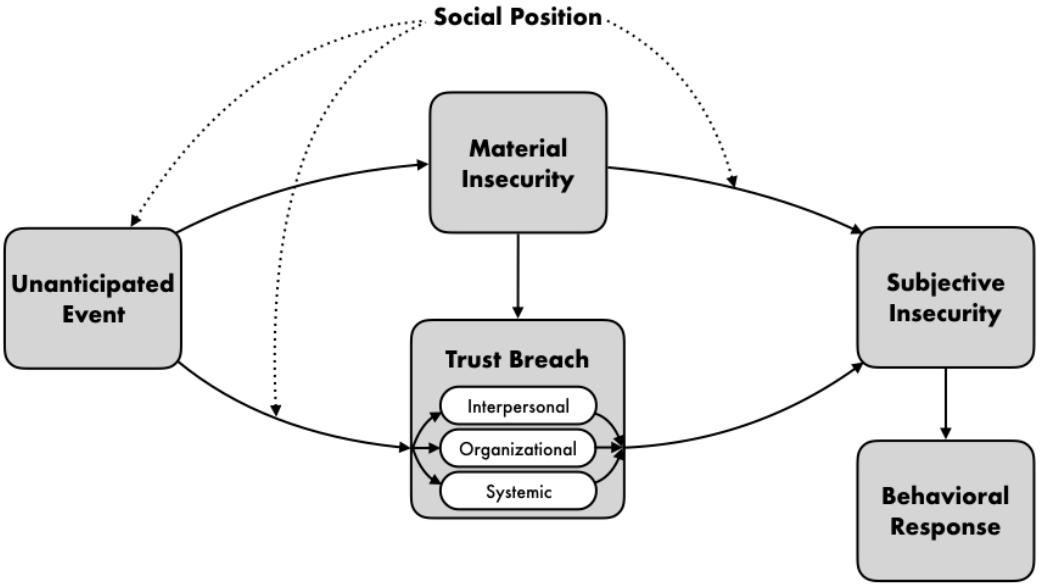

Figure 1. Trust-Based Model of Insecurity