

Identity Theft at the Intersection of Citizenship and Ethnicity Before and During the COVID-19 Pandemic: A Design-Correct Replication and Extension Using the National Crime Victimization Survey

Asim Uludag

auludag@emich.edu

Eastern Michigan University

Bilal Sevinc

Michigan State University

Cooper Maher

Michigan State University

Halil Bisgin

University of Michigan–Flint

Suleyman Uludag

University of Michigan–Flint

Research Article

Keywords: identity theft, citizenship, Hispanic ethnicity, COVID-19 pandemic, routine activity theory, system avoidance

Posted Date: October 14th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11197993/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.
[Read Full License](#)

Additional Declarations: No competing interests reported.

Identity Theft at the Intersection of Citizenship and Ethnicity Before and During the COVID-19 Pandemic: A Design-Correct Replication and Extension Using the National Crime Victimization Survey

Anonymized for Review^{1*}

^{1*}Submission to Security Journal.

Abstract

Identity theft cost 23.9 million U.S. victims \$16.4 billion in 2021. Analysis of the 2018 NCVS Identity Theft Supplement found lower victimization odds for noncitizens than citizens and for Hispanic than non-Hispanic persons, but elevated risk for Hispanic noncitizens beyond either alone. Whether this held during the pandemic, when benefit programs required institutional engagement many noncitizens had avoided, was unknown. We replicate and extend this analysis with 2018 and 2021 data, adding the weights and design-correct standard errors it lacked. The Hispanic protective effect was stable. The noncitizen effect lost significance in 2021, but no cross-wave change was significant. The doubly marginalized interaction replicated only under the original method and was null in 2021. Benefits fraud among victims surged, with implications for emergency-program identity verification.

Keywords: identity theft, citizenship, Hispanic ethnicity, COVID-19 pandemic, routine activity theory, system avoidance

1 Introduction

Identity theft is among the most prevalent and costly cybercrimes affecting U.S. consumers: an estimated 23.9 million people were victimized in 2021 alone, with total losses of \$16.4 billion (Harrell and Thompson 2023). Beyond direct financial loss, victims face the burden of restoring compromised accounts and credit records, procedural friction with financial institutions and government agencies, and documented emotional and behavioral-health harm that is distinct from, and additive to, the financial loss itself (Maher and Hayes 2024). For security practitioners and policymakers, identity theft is also unusual among cybercrimes in how directly it depends on institutional design: exposure is shaped not only by an individual’s own online behavior but by how financial institutions, credit bureaus, and government benefit programs verify identity before granting access to accounts, credit, or emergency funds. When those verification systems are strained, as they were during the COVID-19 pandemic’s rapid deployment of emergency benefit programs (U.S. Government Accountability Office 2024), which population is most exposed to the resulting gaps is an empirical question with direct implications for how such systems should be designed.

Research on immigration and crime finds that immigration does not increase crime and is, on balance, weakly associated with lower crime rates (Zatz and Smith 2012; Ousey and Kubrin 2018). National victimization data, which have recorded citizenship only since 2017, point in a similar direction for direct-contact crime: immigrants and noncitizens generally face lower victimization risk than native-born citizens (Xie and Baumer 2021; Kemper and Kolker 2023), the so-called immigrant protective effect, often attributed to system-avoidance behaviors driven by fear of immigration consequences (Fussell 2011). Whether the same pattern, and the same mechanism, extends to identity theft is less clear, because identity theft differs structurally from direct-contact crime in ways that could plausibly weaken or reverse a protective effect built on system avoidance. There is no co-presence with an offender; exposure is mediated

by an individual’s digital footprint, financial account holdings, and the institutions that hold and share personal information; and recognition of victimization depends on account monitoring and institutional notification pathways that themselves vary by trust in, and engagement with, those institutions. A behavior that protects against direct-contact crime, avoiding institutional contact, could plausibly leave a thinner digital and financial footprint that is also less exposed to identity theft, or it could leave noncitizens less able than citizens to detect and respond to victimization once it occurs. Distinguishing between these possibilities requires evidence specific to identity theft, not an assumption that patterns from direct-contact crime transfer directly.

Maier (2024) provided the first systematic test, using the 2018 NCVS-ITS. Noncitizens had significantly lower odds of past-year identity theft victimization than citizens, and Hispanic respondents independently had lower odds than non-Hispanic respondents; critically, the interaction between the two was positive and significant, indicating that Hispanic noncitizens faced elevated relative risk compared with what either main effect alone would predict. Maier interpreted this doubly marginalized pattern as potentially reflecting the targeting of Hispanic noncitizens by Spanish-language scams that exploit limited English proficiency, compounded by trust-based barriers to protective institutional engagement, such as credit monitoring and fraud reporting, across both marginalized statuses simultaneously. However, the study did not account for the NCVS’s stratified, clustered sampling design: its models were estimated without survey weights and with model-based rather than design-based standard errors, potentially limiting the generalizability of its estimates and overstating their precision (Section 6.3).

The COVID-19 pandemic altered the conditions underlying these patterns at a scale few natural experiments could replicate. Emergency benefit programs, including expanded unemployment insurance, the Paycheck Protection Program, and Economic Impact Payments, required rapid, often remote identity verification at a scale and

speed that outpaced existing fraud-prevention infrastructure; oversight bodies have since estimated between \$100 billion and \$135 billion in fraudulent unemployment insurance payments alone during the pandemic (U.S. Government Accountability Office 2023), with identity theft documented as a primary mechanism across these and other emergency programs (Pandemic Response Accountability Committee 2023). Consumer protection agencies simultaneously documented Spanish-language scams specifically exploiting pandemic-era financial anxiety (Federal Trade Commission 2020). For noncitizen households engaged in the system avoidance associated with the pre-pandemic protective effect, the pandemic forced a choice between continued avoidance and engagement with the very federal systems that avoidance had previously bypassed. Whether this disruption weakened, left unchanged, or reversed the pre-pandemic patterns is an empirical question the 2018 data alone cannot answer.

The 2021 NCVS-ITS (ICPSR 38501), collected July through December 2021, has been used by a small set of studies for adjacent questions. Irvin-Erickson (2024) examined whether immigration status predicted the likelihood of reporting identity theft to law enforcement, finding immigrant-born victims less likely to report than US-born racial and ethnic minority victims. Other work using the same wave has examined victimization risk and the nonfinancial consequences of identity theft victimization, and the extent to which disabilities predict these outcomes (Maher et al. 2025), as well as victims' decisions to engage in protective behaviors following victimization (Maher 2025). None of this work has directly re-tested the citizenship-by-ethnicity victimization-risk pattern Maher (2024) documented, leaving open whether the pre-pandemic pattern, and the theoretical account built around it, still describes the population it was meant to describe.

This study makes two primary contributions, with several supporting analyses developed around them. First, it develops a structural-vulnerability account of why pandemic conditions specifically should be expected to alter these patterns, tracing the

mechanism through system avoidance, institutional-trust pathways, and the doubly marginalized hypothesis, and evaluates that account against a pooled cross-year model that formally tests whether the citizenship and interaction effects differed between 2018 and 2021. Second, it carries that account onto the pandemic-era 2021 wave, which the original analysis predates, disaggregating 2021 results by victimization subtype and documenting a substantial pandemic-era rise in government-benefits fraud among identity theft victims, evidence directly relevant to the design of identity verification in emergency benefit programs. Throughout, estimation applies Taylor-series linearized standard errors that properly account for the NCVS’s stratified, clustered sampling design, a correction the original analysis did not apply.¹

2 Theoretical Framework

2.1 Lifestyle-Routine Activity Theory

Lifestyle-routine activity theory is a framework for understanding opportunity structures for crime events, and reflects an integration of earlier lifestyle-exposure and routine activity theories (Hindelang et al. 1978; Cohen and Felson 1979; see also Cohen et al. 1981). This integrated theory explains that criminal opportunity, and thus victimization risk, is a function of several elements converging in time and space: exposure to crime, a motivated offender, a suitable target, and the absence of a capable guardian. Extended to non-contact, technology-mediated crime (Reyns 2013; Reyns and Henson 2016), the theory’s components take a different form than in the direct-contact crime for which it was originally developed. Motivated offenders are not geographically bounded; a data breach or scam campaign originating anywhere can reach any digitally exposed target. Exposure and target suitability depend on an individual’s digital footprint, financial account holdings, and information-disclosure patterns rather than on physical proximity and accessibility. Capable guardianship is overwhelmingly institutional rather than personal, residing in the fraud-detection systems of banks

and credit bureaus, the verification procedures of government agencies, and the security practices of the platforms an individual uses, rather than in an individual’s own vigilance alone.

Applied to the pandemic period, each component plausibly shifted. Motivated offenders scaled their operations through crime-as-a-service ecosystems and the specific, time-limited opportunity presented by large, rapidly disbursed emergency benefit programs. Exposure and target suitability expanded as households that had previously limited their financial and institutional footprint were required to engage with digital systems, in some cases for the first time, to access remote work, telehealth, online banking, or emergency benefits. Capable guardianship arguably degraded, as institutions under pandemic-era operational strain relaxed identity-verification standards to meet the speed demands of emergency benefit disbursement. Lifestyle-routine activity theory predicts that this combination (greater exposure, more motivated offenders, more suitable targets, and weaker guardianship simultaneously) should increase victimization risk broadly. It does not, on its own, predict how this risk should be distributed across citizenship and ethnicity, which is where the mechanisms below become necessary rather than supplementary.

2.2 System Avoidance and the Deportation-Threat Dynamic

System avoidance describes the tendency of individuals in mixed-status households, or with precarious immigration status, to limit contact with formal institutions (government agencies, financial institutions, even schools and hospitals) out of fear that such contact could expose themselves or family members to immigration enforcement (Patler and Gonzalez 2021). Fussell (2011) documents the deportation-threat dynamic underlying this behavior: the perceived risk of institutional contact is not limited to agencies with direct immigration-enforcement authority, but generalizes to institutions perceived as connected to government surveillance broadly. For identity theft

specifically, system avoidance carries an ambiguous prediction. If avoidance translates into a thinner digital and financial footprint (fewer bank accounts, less credit history, less online engagement), it should reduce target suitability and thus victimization risk, consistent with the protective effect Maher (2024) documented pre-pandemic. But system avoidance could equally leave noncitizens less able than citizens to detect victimization once it occurs, since account monitoring and fraud alerts depend on exactly the institutional engagement avoidance minimizes, and less willing to report or resolve victimization once detected, given the same institutional-trust barriers. The pre-pandemic protective effect is therefore consistent with reduced exposure, reduced detection, or both; the NCVS-ITS, which measures self-recognized victimization, cannot fully distinguish between these explanations, a limitation we return to in the Discussion.

The pandemic tested this mechanism directly. Emergency benefit programs (unemployment insurance, stimulus payments, and pandemic-era rental assistance) required the institutional engagement system avoidance was built to minimize, under economic pressure severe enough to override some households' prior avoidance. That engagement also put applicants' immigration status directly before federal systems: almost all states surveyed by the U.S. Government Accountability Office (2024) reported using the Systematic Alien Verification for Entitlements (SAVE) program to confirm citizenship and immigration status before granting Pandemic Unemployment Assistance, so seeking pandemic benefits meant submitting to precisely the kind of government status check that system avoidance is organized around. If system avoidance underlies the pre-pandemic protective effect, forced pandemic-era engagement should weaken it, consistent with Hypothesis 4 below. This account does not require that all, or even most, noncitizen households participated in pandemic benefit programs, only that an economically meaningful subset did, increasing their institutional footprint relative

to their own pre-pandemic baseline in a way detectable in aggregate victimization patterns. The account therefore predicts a weakened, not eliminated, protective effect.

2.3 The Doubly Marginalized Hypothesis

Maher (2024) proposed that Hispanic noncitizens face a doubly marginalized risk elevation, beyond what either citizenship or ethnicity predicts alone, through two compounding mechanisms. First, language-specific targeting: scammers have documented histories of running Spanish-language campaigns that exploit both limited English proficiency and community-specific trust networks, a pattern consumer protection agencies have flagged specifically in pandemic-era fraud (Federal Trade Commission 2020). Limited English proficiency may also weaken self-protection: in a mixed-method study of a convenience sample of Spanish- and Vietnamese-speaking Internet users with limited English proficiency, Ngo et al. (2026) found that cyber hygiene practices predicted several forms of cyber victimization, that participants' knowledge of recommended practices was inadequate, and that they had difficulty finding actionable cybersecurity guidance in their own languages. Second, compounded institutional-trust barriers: the same system avoidance shaping noncitizens' exposure operates independently for Hispanic ethnicity through documented barriers to protective institutional engagement (credit monitoring and fraud reporting), so holding both statuses could compound rather than merely add their separate effects.

2.4 Synthesis: Predictions Under Pandemic Conditions

These three frameworks generate a coherent set of directional predictions for the pandemic period, stated here before turning to the results. We hold ourselves to reporting each hypothesis's outcome as supported, unsupported, or inconclusive on its own terms, rather than reinterpreting a null result as theory-consistent after the fact. Lifestyle-routine activity theory predicts elevated victimization risk broadly, as exposure, motivated offenders, target suitability, and guardianship all shifted in directions

that favor offenders. System avoidance predicts that any pre-pandemic protective effect tied to noncitizen status should weaken to the extent, and only to the extent, that pandemic conditions forced institutional engagement noncitizens had previously avoided; a fully stable or a fully reversed effect would each be inconsistent with this account, for different reasons. The doubly marginalized hypothesis predicts that Hispanic noncitizens specifically, not noncitizens or Hispanic persons generally, should show the sharpest pandemic-era change, since the language-targeting and compounded-institutional-trust mechanisms are specific to that intersection rather than to either status alone. Our results diverge from that prediction for the interaction term once design-correct standard errors are applied; we treat that divergence as unsupportive of H5 as stated, and separately ask, in the Discussion, whether the underlying mechanism failed to operate as theorized or whether the original finding was more sensitive to estimation method than to the pattern it was interpreted as describing. We do not treat the second possibility as a substitute for reporting the first.

3 Literature Review

3.1 Demographics of Identity Theft Victimization

Identity theft victimization does not distribute evenly across demographic groups. Descriptive work using NCVS-ITS and related sources has documented that raw victimization rates tend to be higher among non-Hispanic White respondents and higher-income households (Anderson 2006; Harrell 2021), a pattern that, read naively, might seem to cut against a structural-vulnerability account. But raw prevalence conflates exposure with detection: higher-income, higher-credit-access households have more accounts to compromise and more monitoring in place to detect compromise, while lower-income and marginalized households may show lower measured prevalence precisely because they have less to monitor and less institutional infrastructure through which victimization becomes visible. Burnes et al. (2020) document a broader

set of risk and protective factors shaping identity theft victimization, and Maher and Hayes (2024) show that nonfinancial consequences (physical and emotional distress and behavioral-health impacts) track loss severity and case-resolution burden in ways a simple financial-loss total misses, underscoring that demographic predictors of identity theft operate through several distinct mechanisms (exposure, detection, and harm) that a single prevalence estimate can obscure.

3.2 Online Routine Activities and Identity Theft

A parallel literature has examined online routine activities as direct predictors of identity theft and related cybercrime, generally finding that online banking, online shopping, social media use, and the extent of an individual’s email account exposure are among the most consistent predictors of victimization risk (Reyns 2013; Reyns and Henson 2016; Akdemir and Lawless 2020). Choi et al. (2021) extend this line of work to show that specific online behaviors shape not only objective exposure but fear of identity theft victimization, a distinction consistent with the target-suitability component of lifestyle-routine activity theory discussed above. This literature provides the behavioral mechanism through which the structural predictors examined here, citizenship and ethnicity, would operate: not directly, but through their association with the online routine activities that determine digital exposure.

3.3 Citizenship, Immigration Status, and Victimization

The relationship between immigration status and victimization has been studied most extensively for direct-contact crime, where the immigrant protective effect appears in national survey data (Xie and Baumer 2021; Kemper and Kolker 2023); a parallel Latino paradox appears in offending outcomes, where Wright et al. (2016) found Hispanic youth reoffending less than socioeconomic risk factors alone would predict. Extension of this literature to non-contact financial crime is comparatively recent.

Irvin-Erickson (2023) tested a four-category citizenship typology (US-born, naturalized citizen, noncitizen, ambiguous status) against identity theft risk using the same 2018 ITS wave, without an ethnicity term; controlling for demographics, neither naturalized citizens nor noncitizens differed significantly from US-born citizens, though the small “ambiguous status” subgroup did, and Maher (2024), reviewed in detail above, provided the first formal test of the citizenship-by-ethnicity interaction that this study re-examines.

3.4 Pandemic-Era Cybercrime and Fraud

Beyond identity theft specifically, a broader literature documents that the pandemic reshaped cybercrime and fraud markets generally. Kemp et al. (2021) document shifts in reported cybercrime and fraud victimization during the pandemic’s early months, Zhang et al. (2022) examine pandemic-era shifts in online fraud targeting more broadly, and Payne (2020) situates COVID-19-era fraud within the broader criminological literature on crime opportunity during large-scale disasters. Over a longer horizon, Engle et al. (2026) find in FBI Internet Crime Complaint Center data for 2015–2024 that cyber-enabled crime, such as fraud, grew significantly in 2020, although they treat the pandemic’s causal role as an open empirical question. Government oversight bodies have quantified the scale of pandemic-benefit fraud specifically: the U.S. Government Accountability Office (2023) estimates between \$100 billion and \$135 billion in fraudulent unemployment insurance payments during the pandemic, and the Pandemic Response Accountability Committee (2023) documents identity theft as a primary mechanism across unemployment insurance, the Paycheck Protection Program, and Economic Injury Disaster Loan programs. This literature establishes that pandemic-era fraud at scale is well documented; what it has not yet established is how that scale of fraud distributed across the citizenship and ethnicity lines this study examines.

3.5 Research Using the 2021 NCVS-ITS

The 2021 NCVS-ITS, released by the Bureau of Justice Statistics in 2023 (Harrell and Thompson 2023), has been used by a small but growing set of studies. Irvin-Erickson (2024) examines reporting behavior rather than victimization risk, finding immigrant-born victims less likely than US-born racial and ethnic minority victims to report identity theft to law enforcement. Other recent work using the same wave has examined victimization risk and the nonfinancial consequences of identity theft victimization, and the extent to which disabilities predict these outcomes (Maher et al. 2025), as well as victims’ decisions to engage in protective behaviors following victimization (Maher 2025). None of this work directly re-tests the citizenship-by-ethnicity victimization-risk pattern under design-correct estimation, the gap this study addresses.

4 Hypotheses

Drawing on the theoretical framework above, we derive five hypotheses. The first three constitute a direct replication of Maher (2024); the final two constitute the pandemic-era extension motivated by the system-avoidance and doubly marginalized mechanisms detailed in Section 2. We then state one further expectation, about victimization subtypes, that the data allow us to examine as a supplemental analysis but not to test formally.

Replication Hypotheses

If the pre-pandemic patterns Maher (2024) documented reflect stable features of identity theft exposure rather than an artifact specific to 2018 conditions, they should reappear in 2021 data despite the intervening disruption.

- **H1:** Noncitizens will face significantly lower odds of past-year identity theft victimization than citizens in 2021, replicating the 2018 finding.

- **H2:** Hispanic respondents will face significantly lower odds of past-year identity theft victimization than non-Hispanic respondents in 2021, replicating the 2018 finding.
- **H3:** Hispanic noncitizens will face elevated relative risk compared with noncitizens or Hispanic persons individually (a positive, significant interaction), replicating the doubly marginalized pattern.

Pandemic-Extension Hypotheses

The system-avoidance account developed in Section 2 predicts that forced pandemic-era institutional engagement should specifically weaken, not eliminate, the noncitizen protective effect, while the doubly marginalized hypothesis predicts the sharpest pandemic-era change should concentrate in the citizenship-by-ethnicity interaction rather than in either main effect alone.

- **H4:** The protective effect of noncitizenship will be *attenuated* in 2021 relative to 2018, consistent with forced digital and institutional migration expanding target suitability for noncitizen populations.
- **H5:** The Hispanic $\times$ Noncitizen interaction will be *strengthened* in 2021 relative to 2018, consistent with documented targeting of Latino immigrant communities by pandemic-benefit scams.

Supplemental Analysis: Victimization Subtypes

If pandemic-era change operates through the emergency-benefit exposure channel specifically, rather than through a general increase in digital exposure, the 2021 citizenship and interaction effects should concentrate in new-account fraud and other misuse of personal information, the subtypes most directly linked to pandemic-benefit fraud, rather than in existing-account misuse. We examine this expectation as a supplemental analysis rather than as a formal hypothesis: testing whether effects *shifted* toward these subtypes would require subtype-specific models in both waves, and we

estimate subtype models for 2021 only (Section 6.5). The subtype results therefore characterize where the 2021 citizenship-by-ethnicity pattern concentrates; they do not test whether that pattern changed from 2018.

5 Data and Methods

5.1 Data Sources

We use the 2018 and 2021 waves of the National Crime Victimization Survey Identity Theft Supplement (NCVS-ITS). The 2018 wave (ICPSR 37923) was collected January through June 2018; the 2021 wave (ICPSR 38501) was collected July through December 2021. Both are publicly available through ICPSR under standard terms of use. The 2018 file was harmonized by ICPSR in a 2023 update (v2) that aligned variable naming across the 2016, 2018, and 2021 waves. The NCVS-ITS is a nationally representative survey that employs a stratified, multi-stage cluster sampling design to survey respondents regarding a range of themes, including experiences with identity theft victimization, consequences and outcomes experienced by victims, and behavioral practices and experiences which may influence individuals' risk of identity theft victimization. Within the 2018 wave, 102,418 individuals completed the NCVS-ITS, relative to 93,308 in 2021.

5.2 Comparability of the 2018 and 2021 Waves

Direct comparison across waves is complicated by four documented instrument changes (Harrell and Thompson 2023). First, the 2021 outcome screeners capture confirmed use of personal information only, while the 2018 screeners captured both attempted and completed incidents; this means the 2018 denominator for several outcomes includes attempted incidents the 2021 denominator excludes. A matched-definition 2018 measure cannot be constructed from the public-use file: the flag variables associated with the 2018 outcome screeners (`VS012F`, `VS017F`, `VS020`, `VS042`, and `VS064`) record only

whether a response was edited during post-collection review, not whether an incident was attempted or completed. Second, the 2021 ITS introduced a dual reference-period design, screening for both lifetime and past-year victimization, which changes how non-victims are routed through the instrument relative to 2018. Third, the 2021 wave newly collects the month and year of the most recent incident, a variable with no 2018 counterpart. Fourth, the 2021 wave added a dedicated screener for email and social-media account misuse, a form of exposure the 2018 instrument did not separately capture. Beyond instrument changes, the two waves were fielded in different, non-overlapping parts of the calendar year (January-June 2018 versus July-December 2021), and pandemic-era conditions shifted NCVS interviewing modes toward telephone administration. Where these changes plausibly affect a specific comparison, we flag the affected estimate directly rather than treating the two waves as a strictly comparable panel.

5.3 Sample

Both analytic samples are restricted to respondents age 16 or older who completed the ITS supplement ($VS008 \in \{1, 2\}$: personal or telephone interview). Household income uses BJS’s *allocated* variable ($V2026A$), as the original analysis also does. For age we use $V3014$ rather than the $V3013$ item the original employs: the two agree wherever both are valid, but $V3013$ carries an out-of-universe code that the original sets to missing, needlessly discarding cases. Education code 27 (“12th grade, no diploma”) is classified below high-school completion, not as graduation; residue codes on education, marital status, and race are treated as missing rather than folded into reference categories; and no respondent is excluded on gender-identity response.² Of the 102,418 (2018) and 93,308 (2021) ITS completers, listwise deletion of respondents missing citizenship, ethnicity, the outcome, or any control variable leaves corrected adjusted analytic samples of $N = 101,389$ and $N = 92,211$, respectively.

5.4 Measures

5.4.1 Outcome Variable

Past-year identity theft victimization (binary) is constructed as the union of existing-account misuse, new-account misuse, and other misuse of personal information, replicating Maher’s (2024) outcome construction. Among confirmed ITS completers, a code indicating the respondent was routed past a given screener because they reported never experiencing that type of incident is recoded as a legitimate negative response (not a victim) rather than as missing data.

5.4.2 Primary Predictors

Citizenship is coded as a binary noncitizen indicator. Hispanic ethnicity is coded as a binary indicator per BJS convention, separate from race. The $\text{Hispanic} \times \text{Noncitizen}$ interaction term is the product of the two.

5.4.3 Control Variables

Models include age, sex, race (Black or Other/multiracial, White as reference), educational attainment (less than high school, high school or GED, some college, bachelor’s degree or higher as reference), marital status, household income, metropolitan statistical area status (suburban or central city, non-MSA as reference), and U.S. Census region (Midwest, South, or West, Northeast as reference). This extends Maher’s (2024) control set (age, education, income, marital status, gender, and race) with urbanicity and region, enters education as categories rather than an ordinal scale, and omits the original model’s five protective-behavior controls, for reasons given in Section 6.3.

5.4.4 Additional Outcome Measures

Two further measures are analyzed. The email and social-media account-misuse screener (VS017E, past-12-months misuse of an email or social-media account) is new

in 2021 and has no 2018 counterpart (Section 6.7). The government-benefits fraud item (VS075), asked in both waves of respondents who reported other misuse of personal information, identifies those whose information was used to fraudulently apply for government benefits (Section 6.6). The 2021 wave also records the timing of each subtype’s most recent incident, which we do not analyze here (Section 7.5).

5.5 Analytic Strategy

All models are estimated using Taylor-series linearized standard errors via `svyglm` in R’s `survey` package (Lumley 2004), declaring the NCVS’s pseudostratum (V2117) and half-sample (V2118) variables as the variance estimation structure and using the ITS final weight (VS363). This is the field-standard approach for complex probability samples such as the NCVS and produces design-based, rather than model-based, standard errors; the `quasibinomial` family is used because weighted outcomes are non-integer and does not alter the point estimates or the design-based standard errors.

The analysis proceeds in six steps. First, weighted descriptive statistics are computed for both waves and compared. Second, the replication model, matching Maher’s (2024) specification, is estimated on the 2021 sample and, as a direct replication check, on the 2018 sample. Alongside the design-correct estimates, we report the identical specification estimated with ordinary, model-based standard errors on the same sample, which isolates what changes when standard-error methodology changes while holding the sample and point estimates fixed. Third, a pooled 2018-2021 model is estimated with a year indicator, the primary predictors, and three year-by-predictor interaction terms ($\text{year} \times \text{noncitizen}$; $\text{year} \times \text{Hispanic}$; $\text{year} \times \text{Hispanic} \times \text{noncitizen}$), with the joint significance of the interaction terms assessed via a Wald test. Fourth, as the supplemental analysis described in Section 4, separate models are estimated for each of the three victimization subtypes on the 2021 sample, plus a fourth, 2021-only subtype model for email/social-media account misuse, with Holm correction applied

separately within each coefficient family (noncitizen, Hispanic, and interaction) across the four subtype models. Fifth, the conditional prevalence of government-benefits fraud among other-misuse victims is compared across waves. Sixth, as a robustness check independent of the standard-error question addressed above, the primary adjusted model is re-estimated on the 2021 sample with standard errors clustered at the household level (V2002) rather than the official pseudostratum/half-sample design, to assess whether within-household correlation not explicitly modeled by the primary design materially changes inference.

5.6 Reproducibility

All analytic code (R `svyglm` scripts and Python data-preparation scripts) will be deposited in a public repository with a citable DOI upon acceptance. Both datasets are publicly available at no cost through ICPSR under standard terms of use requiring registration.

6 Results

6.1 Sample Descriptives

The 2021 sample is somewhat smaller than 2018 ($N = 92,211$ versus $N = 101,389$) and shows a modestly lower weighted past-year victimization prevalence (7.71% versus 9.29%, $p < .001$), though the instrument changes described in Section 5.2 mean this difference should not be read as a like-for-like decline. The weighted Hispanic share of the sample was 16.36% in 2018 and 17.08% in 2021, and the noncitizen share was 5.77% and 5.39%; neither difference is statistically significant (Hispanic $p = .157$; noncitizen $p = .074$).³

6.2 Replication: Design-Correct Estimation, 2018 and 2021

Table 1 reports the replication model with design-correct, Taylor-series linearized standard errors, in both waves, on the corrected analytic samples described in Section 5.

Table 1 Citizenship, Ethnicity, and Identity Theft Victimization, Design-Correct Estimation, 2018 and 2021

Variable	2018 ($N = 101,389$)	2021 ($N = 92,211$)
Noncitizen (OR, 95% CI)	0.69 [0.57, 0.83]	0.89 [0.74, 1.07]
Hispanic (OR, 95% CI)	0.79 [0.71, 0.87]	0.76 [0.69, 0.84]
Hisp. $\times$ Noncit. (OR, 95% CI)	1.33 [0.98, 1.81]	0.89 [0.60, 1.32]
Interaction p	.070	.56

The Hispanic main effect is significant in both waves; the noncitizen main effect is significant in 2018 but not in 2021 ($p = .20$). The Hispanic $\times$ noncitizen interaction is positive and marginal in 2018 ($p = .070$) and near null in 2021 ($p = .56$). This pattern, present but weaker in 2018 than the original published estimate and absent by 2021, motivated a direct reconciliation with the original study.

6.3 Reconciling Sample Construction with the Original Study

Our 2018 analytic sample ($N = 101,389$) is substantially larger than Maher’s (2024) reported $n = 71,984$, and the difference has to be accounted for before any cross-wave comparison can be interpreted. The companion short report reconstructs the original sample step by step from the author’s own analysis code and locates the discrepancy in a single missing-data convention: an outcome-screener skip code, which a respondent receives only when prior routing has already established non-victimization for that component, is treated as missing rather than as a negative response. Because the components are summed, this drops every respondent routed past any one of them. The practical effect in the 2018 instrument is to restrict the analysis to respondents holding

both a bank account and a credit card. That reading is corroborated independently: Irvin-Erickson (2023), analyzing the same wave without this convention, reports $N = 99,295$, close to ours and far from the original. We adopt the larger sample throughout, and reproduce the original construction here only to establish that the two analyses can be reconciled exactly.

Table 2 Hispanic $\times$ Noncitizen Interaction, 2018, on the Reconstructed Original Sample ($N = 71,984$): Estimator Decomposition

Estimator	N	OR	95% CI	p
Unweighted, model-based SE (original method)	71,984	1.38	[1.01, 1.88]	.042
Survey-weighted, model-based SE	71,984	1.47	[1.12, 1.93]	.005
Survey-weighted, Taylor-linearized SE	71,984	1.47	[1.00, 2.18]	.052

Wald intervals, as in the original study. Row 1 recovers the published estimate to its reported precision. The coefficient is identical in rows 2 and 3, which differ only in how its covariance is computed. All three rows retain the original specification, including the five protective-behavior controls.

Table 2 isolates what changes, and what does not, when the original author’s exact sample construction is held fixed. Row 1 reproduces his published estimate exactly, on both sample size and coefficient: the reconciliation is complete on his own terms. Moving from unweighted to survey-weighted estimation, a correction his original analysis did not apply, shifts the point estimate (OR 1.38 to 1.47); holding that weighted specification fixed, replacing model-based standard errors with design-correct ones, a second correction his analysis did not apply, widens the interval from [1.12, 1.93] to [1.00, 2.18], so that a p of .005 becomes .052 at an unchanged coefficient. The interval now includes 1, if barely.

The same pattern holds on our corrected 2018 sample, where the interaction is significant with survey weights and model-based standard errors (OR = 1.33, $p = .019$) but not with design-correct ones ($p = .070$). A full crossing of sample construction against covariate specification and estimator, reported in the companion short report, leaves the weighted point estimate stable across every combination examined (OR

1.27 to 1.49). For present purposes the relevant conclusion is narrower: the published interaction replicates exactly under the original method, and the 2018 estimate is specification-sensitive thereafter, so the pandemic-era comparison developed below is drawn against a 2018 baseline that is itself uncertain rather than against a settled parameter.

6.4 Pooled Cross-Year Model

The pooled model’s year main effect ($OR = 0.79$, $p < .001$) confirms an overall decline in identity theft prevalence between waves. None of the three year-by-predictor interaction terms reached significance: year $\times$ noncitizen ($OR = 1.18$, $p = .19$), year $\times$ Hispanic ($OR = 0.94$, $p = .38$), and the triple interaction ($OR = 0.76$, $p = .28$); the joint Wald test confirmed the three interaction terms did not collectively differ from zero ($F = 1.14$, $df = 3$, $p = .34$). H4’s predicted attenuation of the noncitizen effect is directionally consistent with the observed shift from significant in 2018 to non-significant in 2021 (Table 1), but the formal cross-year test provides no statistical support for concluding this shift is reliable rather than sampling variation. H5’s predicted strengthening of the interaction is not supported in either direction; if anything the point estimate moves toward null.

6.5 Supplemental Analysis: Victimization Subtypes

Disaggregating the 2021 results by victimization subtype (existing-account misuse, new-account fraud, other misuse, and email/social-media misuse, Section 6.7), the Hispanic protective effect on existing-account misuse is robust ($OR = 0.74$, $p_{Holm} < .001$), and on email/social-media misuse both the Hispanic ($OR = 0.72$, $p_{Holm} = .013$) and noncitizen ($OR = 0.49$, $p_{Holm} = .032$) effects survive correction; no other main effect survives Holm correction within its family across the four subtype tests. The Hispanic $\times$ Noncitizen interaction for new-account fraud shows $OR = 2.54$, but rests on

only four Hispanic noncitizen victims out of 2,026 respondents (0.2%); this single-digit event count precludes meaningful inference. Because these models are estimated for 2021 only, they characterize where the 2021 pattern concentrates rather than testing a shift from 2018 (Section 4), and this cell size means even that cross-sectional reading would be unreliable for new-account fraud specifically. None of the four subtype interaction terms (existing-account OR = 0.77, new-account OR = 2.54, other-misuse OR = 1.94, email/social OR = 1.70) survives Holm correction ($p_{\text{Holm}} = .62$ for all four).

6.6 Pandemic Signal: Government-Benefits Fraud

Among respondents who reported other misuse of personal information, the weighted share reporting that information was used to fraudulently apply for government benefits rose from 12.1% in 2018 to 78.8% in 2021 (unweighted: 15.8%, 64 of 405, versus 81.3%, 737 of 907). A documented instrument change bears on this comparison directly: the 2018 screeners, including the benefits-fraud item, captured attempted as well as completed incidents, while the 2021 screeners captured completed incidents only. Because attempted incidents can enter both the numerator and the denominator of this share, the direction of the resulting bias cannot be signed with public-use data; the comparison indicates a large shift, not its precise magnitude. This shift is consistent with independently documented evidence on pandemic-benefit fraud at scale (U.S. Government Accountability Office 2023; Pandemic Response Accountability Committee 2023), though the available data do not permit breaking this specific comparison out by citizenship or ethnicity; that limitation is addressed directly in Section 7.3.

6.7 Email and Social-Media Account Misuse

The 2021-only email and social-media account-misuse screener (VS017E) identifies 2,123 victims among the corrected 2021 sample (2.30% unweighted), a subtype with an exposure pathway, credential compromise rather than direct financial-account access,

distinct from the three subtypes examined above. Screener code 9 (routed past the item as a lifetime non-victim) is recoded as a legitimate negative response here as elsewhere in this paper. The resulting $N = 92,213$ is two more than the primary analytic sample, because two respondents with a residue code on another outcome screener have a valid response on this one. Table 3 reports the same design-correct specification estimated on this outcome.

Table 3 Email and Social-Media Account Misuse: Design-Correct Estimation, 2021 ($N = 92,213$)

Variable	OR	p
Noncitizen	0.49	.008
Hispanic	0.72	.004
Hispanic $\times$ Noncitizen	1.70	.156

Both main effects are protective and more pronounced than in the primary outcome (Table 1): relative to citizens and non-Hispanic respondents, respectively, noncitizens and Hispanic respondents each face substantially lower odds of email/social-media account misuse specifically, and both effects survive Holm correction across the four subtype tests (Section 6.5). The interaction is positive but not significant ($OR = 1.70$, $p = .156$). It is directionally consistent with the doubly marginalized hypothesis, but as a 2021-only estimate it cannot show whether that pattern changed from 2018. Unlike the new-account fraud interaction reported in Section 6.5, this estimate is not built on a single-digit event count: 23 Hispanic noncitizen respondents report email or social-media account misuse, out of 2,026 Hispanic noncitizen respondents in the 2021 sample. This is still a modest cell for a three-way comparison, and the estimate should be read as suggestive at most.

6.8 Robustness Check: Household-Clustered Standard Errors

The corrected 2021 analytic sample contains 92,211 respondents in 48,501 unique households (1.90 people per household on average), enough within-household structure for a meaningful comparison. Re-estimating the primary adjusted model with standard errors clustered on household (V2002) rather than the official pseudostratum/half-sample design leaves every coefficient exactly unchanged (household clustering changes only the variance calculation) and leaves every conclusion materially unchanged: the Hispanic effect remains significant under both designs ($p < .001$), the noncitizen effect remains non-significant under both ($p = .20$ official versus $p = .29$ household-clustered), and the interaction term remains non-significant under both ($p = .56$ official versus $p = .54$ household-clustered).

7 Discussion

7.1 What Replicated, and What Did Not

Stated against the hypotheses in Section 4: H1 is not supported (the 2021 noncitizen effect is non-significant, $OR = 0.89$, $p = .20$); H2 is supported; H3 is not supported (2021 interaction $OR = 0.89$, $p = .56$); H4 is directionally consistent with the point estimates but not supported by the pooled cross-year test; and H5 is not supported. The supplemental subtype analysis (Section 6.5), a 2021-only characterization rather than a test of change, is inconclusive: no subtype interaction survives Holm correction, and the new-account estimate rests on four Hispanic noncitizen victims.

The Hispanic protective effect is the most robust finding across both waves and both standard-error methods: Hispanic respondents consistently faced lower odds of identity theft victimization relative to non-Hispanic respondents, a result that held under pandemic conditions and was not sensitive to variance-estimation choices. This stability is consistent with the lifestyle-routine activity account developed in

Section 2: whatever mechanism produces lower baseline exposure among Hispanic than non-Hispanic respondents, potentially including closer in-group financial networks, particular online behavior patterns, or targeted vigilance in specific domains, was not materially disrupted by the pandemic’s broad shift in target suitability and guardianship.

The noncitizen protective effect weakened from significant in 2018 to non-significant in 2021, directionally consistent with H4’s system-avoidance account, but the pooled model’s formal cross-year test does not support treating this shift as statistically reliable rather than sampling variation. This is a genuinely different conclusion than either “the pandemic clearly weakened noncitizens’ protection” or “the pandemic had no effect”: the point estimates move in the theoretically predicted direction, consistent with partial disruption of system avoidance among the subset of noncitizen households that engaged with emergency benefit programs, but the evidence does not meet the threshold to state that conclusion with confidence.

The doubly marginalized interaction is not simply supported or refuted; it is fragile in a specific, now well-characterized way (Section 6.3). On Maher’s (2024) exact original sample, obtained directly from the author and replicated to the case, the interaction is significant under his method ($OR = 1.38$, $p = .042$) and under survey-weighted estimation with model-based standard errors ($OR = 1.47$, $p = .005$), but does not reach significance at the conventional $\alpha = .05$ threshold once design-correct variance estimation is applied to that same sample ($OR = 1.47$, $p = .052$), though its 95% confidence interval includes 1 only barely. On our independently corrected, substantially larger sample it is smaller and only marginal in 2018 ($p = .070$) and effectively absent in 2021 ($p = .56$). More precisely, the corrected 2018 estimate is specification-sensitive rather than simply marginal: it regains nominal significance under survey-weighted model-based standard errors ($p = .019$) or with the original study’s protective-behavior controls added ($p = .031$); 2021 remains null under every

specification tried. What separates these verdicts is chiefly the variance estimator. Across the original and corrected samples and covariate specifications, survey-weighted estimates with model-based standard errors are uniformly significant while design-correct estimates rarely are, and restricting our corrected data to the population the original construction retains barely moves the estimate (Section 6.3). The missing-data convention that removed 26,824 cases explains the difference in sample size, not the difference in significance. This does not mean the doubly marginalized hypothesis is falsified. The point estimate is stable (OR 1.27 to 1.49 across 2018 specifications), but its uncertainty under the survey design is wide enough that a modest, possibly wave-specific effect cannot be distinguished from none. The exercise illustrates a documentation practice worth adopting more broadly in survey-based cybercrime research: analytic sample construction, specifically missing-data recoding of skip-routed items, should be reported precisely enough that a discrepancy between independent analyses of the same public-use file can be diagnosed without contacting the original author, and design-correct standard errors should be reported alongside model-based ones for any complex-survey interaction effect, since the two can disagree at exactly the threshold that determines a finding’s interpretation.

7.2 Theoretical Implications

Judged on their own terms, as Section 2 committed to, the three frameworks receive limited support. Lifestyle-routine activity theory’s prediction of broadly elevated pandemic-era risk is not supported: weighted prevalence fell from 9.29% to 7.71% (pooled year OR = 0.79). Part of that decline may be mechanical, since the 2018 screeners counted attempted incidents the 2021 screeners did not, and countervailing forces such as reduced offline exposure during lockdowns may also contribute, but neither possibility turns the decline into support for the prediction. The system-avoidance account’s prediction of a partial disruption of the noncitizen protective

effect matches the direction of the point estimates but is not supported by the formal cross-year test. The doubly marginalized hypothesis (H5) is not supported, and the pre-pandemic interaction it builds on is better described as imprecisely estimated than as refuted (Section 6.3). Either the language-targeting and compounded-trust mechanisms operate more weakly, or more narrowly, than the original estimate suggested, or they operated under 2018 conditions and did not persist into the pandemic-era wave; later waves can adjudicate between these. The email/social-media subtype result (Section 6.7) points the same way: its interaction is positive but not significant ($OR = 1.70$, $p = .156$), so it offers no evidence of a subtype-concentrated doubly marginalized mechanism.

7.3 Policy and Practical Implications

Multilingual fraud-prevention outreach. The stability of the Hispanic protective effect across waves does not diminish the case for multilingual outreach, which rests not on elevated measured risk but on documented Spanish-language targeting in pandemic-era scams (Federal Trade Commission 2020) and on barriers to reporting and recovery once victimization occurs. Internet users with limited English proficiency appear motivated to adopt recommended cyber hygiene practices but report difficulty finding step-by-step guidance in their own languages (Ngo et al. 2026), so in-language prevention materials and fraud-reporting forms may reach a receptive audience. Financial institutions and government agencies deploying fraud-awareness communications should audit whether Spanish-language materials adequately cover pandemic-benefit and emergency-program identity theft specifically, not only the phishing and account-takeover scenarios such materials typically emphasize.

Emergency-program identity verification. The government-benefits fraud shift documented in Section 6 is consistent with rapid deployment of pandemic-era benefit

programs creating identity-verification gaps that fraudsters exploited at scale. We caution that this shift coincides with broader pandemic-era changes, including accelerated digital adoption and shifting fraud-market dynamics, any of which could contribute; the data do not permit isolating citizenship- or ethnicity-specific benefits-fraud rates, so we do not claim this channel disproportionately affected noncitizen or Hispanic households, only that it merits identity-verification attention regardless of which population it affected most. With that caveat, emergency-program designers should treat identity verification as a priority security requirement from program launch, not a feature added after fraud losses are documented, and should design verification pathways that do not inadvertently exclude noncitizen-headed or mixed-status households, a failure mode that would simultaneously increase fraud exposure for those households and reduce their access to legitimate benefits.

Fraud-detection systems and under-reporting. Machine-learning fraud-detection systems trained on historical reported-case data can systematically underweight victimization patterns in populations with low reporting baselines. Undocumented immigrants specifically have been shown to underuse formal help and reporting channels after victimization (Zadnik et al. 2016), and NCVS-ITS data capture only self-recognized victimization, itself less likely among victims who engage least with the credit-monitoring and account-alert tools that make theft visible (Maher 2025). This suggests administrative data on identity theft (fraud reports, credit-dispute filings, law enforcement contacts) may systematically undercount exposure for noncitizen and immigrant populations, and that fraud-detection systems trained on such data can inherit this bias structurally, flagging the populations most visible in the training data rather than the populations at greatest underlying risk. Security teams building or procuring such systems should treat reporting-rate heterogeneity as a design constraint, not an afterthought, when evaluating model fairness and detection recall across demographic groups.

7.4 Limitations

Several limitations bound interpretation of these findings. First, the cross-sectional design of both ITS waves precludes causal inference; the associations documented here are consistent with the proposed mechanisms but do not establish them. Second, the two waves do not constitute a panel: different respondents were surveyed in 2018 and 2021, and between-wave changes in sample composition cannot be fully disentangled from genuine changes in victimization patterns. Third, the four documented instrument changes detailed in Section 5.2 limit comparability, and a matched-definition analysis that would address the most consequential of them is not achievable with the public-use file, since no outcome-item flag variable distinguishes attempted from completed incidents. Fourth, the NCVS-ITS captures only victimization respondents recognize and self-report; if recognition and reporting rates differ by citizenship or ethnicity, plausible given differential institutional engagement, our estimates may not be comparable across groups in the way standard regression assumes. Fifth, pandemic-era effects on identity theft are entangled with simultaneous secular trends in data breaches, digital adoption, and the broader cybercrime ecosystem (Kemp et al. 2021), making it impossible to attribute observed changes exclusively to pandemic conditions. Sixth, small cell sizes for key subgroups are severe: the Hispanic $\times$ Noncitizen new-account fraud cell contains only four victims out of 2,026 Hispanic noncitizen respondents, and the corresponding odds ratio reflects single-digit event-count noise rather than a systematic association. Seventh, the subtype analysis involves four simultaneous outcomes; applying Holm correction within the interaction-term family, none of the four survives, while within the main-effect families the Hispanic effects on existing-account and email/social-media misuse and the noncitizen effect on email/social-media misuse survive. Eighth, the pooled cross-year model’s year-by-predictor interaction terms are subject to measurement non-equivalence bias from the

instrument changes documented above; lacking grounds to sign that bias in either direction, we read these terms as suggestive, not precise.

7.5 Directions for Future Research

When a subsequent ITS wave is released, repeating this analysis with a post-pandemic recovery time point would help disentangle pandemic-specific from secular-trend effects, and adding the 2016 wave would extend the pre-pandemic baseline. The 2021 incident-timing variables could test whether victimization clustered in periods of peak benefit disbursement, although no single timing variable spans all three subtypes and the new-account cell is small (586 victims, four of them Hispanic noncitizens). Linkage of the ITS with administrative data (fraud reports, FTC Consumer Sentinel filings, or credit-bureau dispute records) could help quantify the under-reporting bias this discussion flags but cannot directly measure with survey data alone. Qualitative work with immigrant identity-theft victims on detection and reporting pathways would help distinguish the reduced-exposure and reduced-detection explanations for the noncitizen protective effect that Section 2 identifies as observationally similar in this design.

8 Conclusion

This paper replicated and extended Maher’s (2024) citizenship-by-ethnicity analysis of identity theft victimization using the pandemic-era 2021 NCVS-ITS, with design-correct variance estimation as the methodological throughline connecting both contributions. The Hispanic protective effect is the most robust finding, stable across waves and standard-error methods. The noncitizen protective effect weakened to non-significance in 2021, directionally consistent with system avoidance but not statistically confirmed as a reliable shift. The doubly marginalized interaction replicates exactly under the original author’s method but does not reach conventional significance under design-correct estimation on either his exact sample ($p = .052$) or our corrected 2018

sample ($p = .070$), and is null in 2021. The government-benefits fraud signal, a rise from 12.1% to 78.8% of other-misuse victims between waves, is strong descriptive evidence, subject to the instrument change noted in Section 6.6, that pandemic emergency programs became a substantially more prominent identity-theft vector.

For security practitioners, these findings carry a specific lesson about attack surface and crisis response. Emergency programs that prioritize speed over identity-verification security do not merely create fraud losses at scale; they expand the attack surface for whichever populations are forced into new institutional engagement by the crisis itself. Multilingual outreach, identity verification that accommodates mixed-status households, and fraud-detection systems that account for reporting-rate heterogeneity across demographic groups are not optional features of emergency-program design; they are requirements to specify before the next crisis, not retrofit after this one's losses are tallied.

Word count: approximately 7,900 (main text, Sections 1–8, excluding abstract, tables, notes, and references). 30 September 2026.

Notes

¹The sample-construction reconciliation and the full estimator decomposition on the original 2018 sample are reported in a companion short report by the present authors, under concurrent review elsewhere and available to the editor on request; Section 6.3 carries forward only what the present analysis requires.

²Maher (2024) excluded 15 transgender and 42 “none of these” gender-identity respondents under a binary gender coding. We retain them; the exclusion is reproduced only in the reconstruction of the original sample (Section 6.3).

³Design-based Wald tests of the difference in weighted proportions, treating the two waves as independent samples (wave-specific strata and PSUs; 340 design degrees of freedom); Rao–Scott corrected chi-square tests give the same conclusions.

References

- Akdemir, N. and C.J. Lawless. 2020. Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research* 30(6): 1665–1687. <https://doi.org/10.1108/INTR-10-2019-0400> .
- Anderson, K.B. 2006. Who are the victims of identity theft? the effect of demographics. *Journal of Public Policy & Marketing* 25(2): 160–171. <https://doi.org/10.1509/jppm.25.2.160> .
- Burnes, D., M. DeLiema, and L. Langton. 2020. Risk and protective factors of identity theft victimization in the United States. *Preventive Medicine Reports* 17: 101058. <https://doi.org/10.1016/j.pmedr.2020.101058> .
- Choi, J., N.E. Kruis, and K.S. Choo. 2021. Explaining fear of identity theft victimization using a routine activity approach. *Journal of Contemporary Criminal Justice* 37(3): 406–426. <https://doi.org/10.1177/10439862211001627> .
- Cohen, L.E. and M. Felson. 1979. Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44(4): 588–608. <https://doi.org/10.2307/2094589> .
- Cohen, L.E., J.R. Kluegel, and K.C. Land. 1981. Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American Sociological Review* 46(5): 505–524. <https://doi.org/10.2307/2094935> .
- Engle, T.A., S.H. Joo, C. Caudill, C.A. Maher, R.M. Corsello, K. Coe, and J.L. Nedelec. 2026. An examination of cybercrime trends within the United States: Findings from the Internet Crime Complaint Center, 2015–2024. *American Journal of Criminal Justice* 51(4): 942–965. <https://doi.org/10.1007/s12103-025-09885-w> .

- Federal Trade Commission. 2020, December. As scammers leverage pandemic fears, FTC and law enforcement partners crack down on deceptive income schemes nationwide. FTC Press Release.
- Fussell, E. 2011. The deportation threat dynamic and victimization of Latino migrants: Wage theft and robbery. *The Sociological Quarterly* 52(4): 593–615. <https://doi.org/10.1111/j.1533-8525.2011.01221.x> .
- Harrell, E. 2021. Victims of identity theft, 2018: Summary. Technical Report NCJ 256085, Bureau of Justice Statistics.
- Harrell, E. and A. Thompson 2023. Victims of identity theft, 2021. Technical Report NCJ 306474, Bureau of Justice Statistics.
- Hindelang, M.J., M.R. Gottfredson, and J. Garofalo. 1978. *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization*. Cambridge, MA: Ballinger.
- Irvin-Erickson, Y. 2023. How does immigration status and citizenship affect identity theft victimization risk in the US? Insights from the 2018 National Crime Victimization Survey Identity Theft Supplement. *Victims & Offenders* 18(7): 1401–1424. <https://doi.org/10.1080/15564886.2023.2231954> .
- Irvin-Erickson, Y. 2024. Victim-reporting of instrumental identity theft to law enforcement in the United States: An analysis of the impact of immigration status of victims. *American Behavioral Scientist*. <https://doi.org/10.1177/00027642241300922> .
- Kemp, S., D. Buil-Gil, A. Moneva, F. Miró-Llinares, and N. Díaz-Castaño. 2021. Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19. *Journal of Contemporary Criminal Justice* 37(4): 480–501.

<https://doi.org/10.1177/10439862211027986> .

Kemper, N. and A.F. Kolker 2023, January. Improving crime victimization data for noncitizen populations. CRS In Focus IF12316, Congressional Research Service.

Lumley, T. 2004. Analysis of complex survey samples. *Journal of Statistical Software* 9(8): 1–19. <https://doi.org/10.18637/jss.v009.i08> .

Maher, C.A. 2024. Examining the association between citizenship and ethnicity on identity theft risk: Findings from the National Crime Victimization Survey. *American Journal of Criminal Justice* 49(3): 400–421. <https://doi.org/10.1007/s12103-024-09759-7> .

Maher, C.A. 2025. To shred or not to shred: Victims’ decisions to engage in protective behaviors following identity theft victimization. *Crime & Delinquency*. <https://doi.org/10.1177/00111287251363965> .

Maher, C.A. and B.E. Hayes. 2024. Nonfinancial consequences of identity theft revisited: Examining the association of out-of-pocket losses with physical or emotional distress and behavioral health. *Criminal Justice and Behavior* 51(3): 459–481. <https://doi.org/10.1177/00938548231223166> .

Maher, C.A., B.E. Hayes, and R.A. Powers. 2025. Vulnerable identities? Examining the association between disability with risk and consequences of identity theft. *Journal of Criminal Justice* 96: 102333. <https://doi.org/10.1016/j.jcrimjus.2024.102333> .

Ngo, F.T., A. Agarwal, and K. Holman. 2026. Cyber hygiene and cyber victimization among limited English proficiency (LEP) Internet users: A mixed-method study. *Victims & Offenders* 21(5): 969–990. <https://doi.org/10.1080/15564886.2024.2329765> .

- Ousey, G.C. and C.E. Kubrin. 2018. Immigration and crime: Assessing a contentious issue. *Annual Review of Criminology* 1: 63–84. <https://doi.org/10.1146/annurev-criminol-032317-092026> .
- Pandemic Response Accountability Committee. 2023, November. New PRAC working group to combat identity fraud in pandemic response programs and improve victim redress. Pandemic Oversight.
- Patler, C. and G. Gonzalez. 2021. Compounded vulnerability: The consequences of immigration detention for institutional attachment and system avoidance in mixed-immigration-status families. *Social Problems* 68(4): 886–902. <https://doi.org/10.1093/socpro/spaa069> .
- Payne, B.K. 2020. Criminals work from home during pandemics too: A public health approach to respond to fraud and crimes against those 50 and above. *American Journal of Criminal Justice* 45: 563–577. <https://doi.org/10.1007/s12103-020-09532-6> .
- Reyns, B.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): 216–238. <https://doi.org/10.1177/0022427811425539> .
- Reyns, B.W. and B. 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): 1119–1139. <https://doi.org/10.1177/0306624X15572861> .
- U.S. Government Accountability Office 2023, September. Unemployment insurance: Estimated amount of fraud during pandemic likely between \$100 billion and \$135 billion. Technical Report GAO-23-106696, U.S. Government Accountability Office.

U.S. Government Accountability Office 2024, July. Pandemic unemployment assistance: States' controls to address fraud. Technical Report GAO-24-107471, U.S. Government Accountability Office.

Wright, K.A., J.J. Turanovic, and N. Rodriguez. 2016. Racial inequality, ethnic inequality, and the system involvement of at-risk youth: Implications for the racial invariance and Latino paradox theses. *Justice Quarterly* 33(5): 863–889. <https://doi.org/10.1080/07418825.2014.987310> .

Xie, M. and E.P. Baumer. 2021. Immigrant status, citizenship, and victimization risk in the United States: New findings from the National Crime Victimization Survey (NCVS). *Criminology* 59(4): 610–644. <https://doi.org/10.1111/1745-9125.12278> .

Zadnik, E., C. Sabina, and C.A. Cuevas. 2016. Violence against latinas: The effects of undocumented status on rates of victimization and help-seeking. *Journal of Interpersonal Violence* 31(6): 1141–1153. <https://doi.org/10.1177/0886260514564062> .

Zatz, M.S. and H. Smith. 2012. Immigration, crime, and victimization: Rhetoric and reality. *Annual Review of Law and Social Science* 8: 141–159. <https://doi.org/10.1146/annurev-lawsocsci-102811-173923> .

Zhang, Y., Q. Wu, T. Zhang, and L. Yang. 2022. Vulnerability and fraud: Evidence from the COVID-19 pandemic. *Humanities and Social Sciences Communications* 9: 424. <https://doi.org/10.1057/s41599-022-01445-5> .