European Economic Letters
ISSN 2323-5233
Vol 16, Issue 1 (2026)
http://eelet.org.uk

Invisible Authentication, Visible Privacy Costs: The Impact of Frictionless 3DS 2.0 on Consumer Trust, Purchase Completion, and Privacy Concerns in the United States

Himani FNU[1]

[1]Project Manager, Independent Researcher, Chicago, USA Corresponding Email: himani1708@gmail.com

Abstract

One step beyond old methods, 3-D Secure 2.0 changes how people verify payments online – no more constant pop-ups, just quiet checks running behind the scenes. Though faster checkouts often mean more purchases go through, some users worry about what gets tracked when they do nothing at all. Behind this ease lies a web connecting smooth logins, whether buyers feel safe, if deals finish successfully, and unease over unseen data collection. To explore these links among U.S. shoppers, researchers gathered answers from 412 individuals who buy things online. Selection followed a structured method meant to reflect broader shopper patterns across the country. A look at the data shows people know about 3DS 2.0 features, how much they trust smooth login steps, whether they finish buying things online, and how worried they are about private info. Even though easier logins help more purchases go through ($\beta = 0.41$, $p < .001$), those same systems make users feel less safe about their data ($\beta = 0.37$, $p < .001$), which pulls in opposite directions. When tested with deeper math tools, trust plays a mid-level role – linking smoother access to more completed buys (indirect effect = 0.18, $p < .01$), yet worry over privacy slows down that trust build-up (interaction $\beta = -0.22$, $p < .01$). Younger folks, ages 18 to 34, tend to like seamless sign-ins more, still – they're also sharper on when companies gather personal details. This lines up with what firms handling payments, stores selling goods, and rule-makers need to weigh: making checkouts fast without hiding how data moves.

A different kind of checkout rolls through the United States now. Because of 3DS 2.0, logging in feels smoother than before. Buyers seem more at ease when sharing details online. Yet some still hesitate, worried about who sees what they share. Finishing a transaction takes less time these days. Payment steps blend into one quiet flow across sites. Trust builds slowly when people feel control stays with them.

Keywords: 3DS 2.0, frictionless authentication, consumer trust, privacy concerns, purchase completion, online payments, United States

1. Introduction

Right now, how people pay online keeps changing fast. Around the world, money spent shop-ping on the internet went past 5.8 trillion dollars just last year. More buying happens through screens. Alongside that rise comes a growing difficulty – proving real customers are who they say without slowing things down too much. That slowdown? It often makes shoppers leave without finishing their purchase. A system called 3-D Secure started years back when Visa launched it under another name: Verified by Visa. This began around 2001. Its job was to confirm buyers during purchases where the physical card isn't present. Trouble is, version one of this method got complaints. People found it annoying because it relied on fixed passwords. Phones didn't handle it well either. On top of that, many dropped out mid-purchase. Some studies said anywhere from ten to twenty-five percent walked away due to these hurdles.

Starting in 2017, EMVCo rolled out 3-D Secure 2.0 – reframing how verification works by using smarter background checks instead of constant prompts. Hidden behind each pur-chase, a web of signals moves instantly from seller to bank: clues like typing rhythm, phone settings, past buys, where someone's logged in from, even browser habits. Because of this flow, most checkouts now pass quietly when danger levels look low. Silence means approval, no pop-ups needed. If numbers stay under the line, shoppers never notice a thing.

Most people like smoother checkout steps these days, thanks to updates in security checks that cut down on dropped purchases. Yet hardly anyone knows how customers really feel about being checked without seeing it happen first.

These quiet background scans gather tons of habits and details while pretending to help – kinda like locking the door but copying every key behind your back. Experts point out this twist: safety tools acting protective might actually be grabbing too much info, way beyond what users expect they're agreeing to when just buying something online.

One place where this study hits close to home is the United States. While Europe en-forces strict login checks through PSD2 rules, American policy stays hands-off when it comes to verifying online payments (Federal Reserve, 2022). Because of that gap, 3DS 2.0 rolls out based on what businesses want, not legal pushes. Stores and banks push for smoother check-outs – yet no law forces them to be clear about how they handle user data (Hayashi & Moore, 2023).

This paper looks into these specific questions:

- What happens when shoppers go through smooth 3DS 2.0 checks – does it nudge their confidence in digital payments? Because ease might shape belief, yet every click tells a story beyond speed.
- Among U.S. consumers, how does smooth login flow tie into actual checkout follow-through?
- How much does worry about hidden data gathering in 3DS 2.0 affect how smoothly login processes shape user confidence? Though ease of access matters, unseen tracking can shift whether people feel safe. When verification feels seamless, trust might grow – yet only if users believe their info isn't being quietly taken. Behind quick approvals lies uncertainty; knowing what's collected changes reactions. Even slick systems lose credibility when transparency drops. Smoothness helps, sure – but not when secrecy shadows the background. Quiet monitoring alters perception, regardless of speed. Confidence hinges less on convenience alone once privacy fades from view.
- Folks often see smooth logins differently based on age, income, or where they grew up. Sometimes younger users accept quick access more easily than older ones. Where you live might shape how much risk feels normal during sign-in steps. Money background can tilt whether convenience seems worth the trade-off. Each group weighs speed against personal data exposure in their own way.

What happens behind the scenes when logins feel too smooth? That question drives an investigation into how invisible trade-offs emerge with effortless access tools. Instead of just celebrating speed, attention turns toward personal data exposure risks during routine digital sign-ins. Findings come from real-world observations linking tech design to user choices about privacy. This work fits where habits meet software logic – especially moments people skip thinking but still make decisions. Not every outcome shows up right away; some effects linger beneath typical usage patterns.

2. Literature Review

2.1 How 3-D Secure Rules Changed Over Time

Back in 2001, Visa introduced 3-D Secure 1.0 using three parts: one for sellers, one for banks issuing cards, another linking them together – meant to confirm online payments. Still, studies kept showing people struggled with it; Murdoch and Anderson found users tired of reusing the same passwords, stores applying rules unevenly, plus risks from fake sites tricking customers. Then Bena and Cordasco discovered something else – shoppers left their carts behind more often, up 20 to 30 percent when stores used version 1.0.

Instead of fixed rules, 3DS 2.0 uses risk levels to decide how a payment gets confirmed. Information moves smoothly among sellers and banks using three linked servers – one han-dles access control, another directs traffic, the third manages security checks (EMVCo, 2019). When a purchase looks safe, it goes through quietly, skipping pop-ups or codes entirely, so shoppers notice nothing at all (Mastercard, 2022).

2.2 Consumer Trust in Digital Payments

Looking at how people accept new tech helps explain why some feel safe using online pay-ments. Institutional trust plays a big role – things like clear rules and familiar setups make users more likely to click buy. When security feels strong but not overbearing, confidence grows. Too much hassle during login, though, tends to wipe that trust away. What seems se-cure to one person might feel invasive to another, shifting their comfort level fast. Familiar surroundings online act like quiet signals that everything is probably okay.

Yet trust grows in ways still poorly mapped when security hides from sight. Most ideas about trust expect people to notice safeguards around them. Now 3DS 2.0 slips past attention

completely, smooth and unseen, making one wonder – can safety no one feels actually build confidence? Without clear view into how protection works, doubt creeps in. What if vanishing security weakens the very faith it aims to support? Hidden layers might not comfort but confuse instead.

2.3 Privacy Issues and Hidden Data Gathering

Privacy worries around quiet background data gathering show up in different ways. One way comes from Nissenbaum's idea about how context shapes what feels private. Another view arrives through Solove's breakdown of harm types tied to personal exposure. Then there is the balance people try to strike – weighing rewards against risk – which Dinev and Hart named long ago. When payments need checks, 3DS 2.0 slips into smoother mode by pulling device details quietly. It gathers signals like browser setup, where someone appears to be online, how they move across screens, even which add-ons live inside their browser. Time zones tag along too, plus traces of past clicks. EMVCo wrote down these pieces back in 2019. Awareness matters sharply – Martin and Murphy found tension grows if users don't know tracking happens. That lack of notice fits exactly what unfolds during seamless login steps.

Although the ICO flagged issues in 2020, it wasn't just about how much data 3DS 2.0 gathers – more like why so much of it gets sent when less would do. Because American law lacks a broad privacy framework like GDPR, people using smooth login systems rarely know what information slips through behind the scenes. While Europe tightens rules around minimal data use, U.S. users stay mostly in the dark on who sees their details during quick verifications.

2.4 Purchase Finalized and Unfinished Carts

Payment trouble often stops people before they finish buying things online (Baymard Institute, 2023). Trouble at checkout makes shoppers more likely to quit, according to Rajamma and team in 2009. When logins need too many steps, some users just walk away – up to one in five, says Felt's work from 2016. Newer systems like 3DS 2.0 seem smoother: Stripe saw fewer drop-offs in 2023, and Adyen's data two years earlier showed similar trends. Still, those numbers come from companies, not labs, so hidden influences might be shaping results without notice – especially if someone cares deeply about their private info.

2.5 Research Gap

One reason stands out – research has not tested how smooth 3DS 2.0 shapes trust, buying behavior, and worries about data at once under one clear model. Earlier work looked at each piece apart, often tied to older verification methods. What changes now is real-world testing that links ease of checkout, user confidence, finishing purchases, and personal information fears – all drawn from American shoppers.

3. Research Methodology

3.1 Research Design

A snapshot of people's views at one moment guided this work. Chosen because it fits well when checking how folks think and act across wide areas (Creswell & Creswell, 2018), the method maps patterns without time shifts. Distance between participants mattered less once numbers shaped the picture clearly.

3.2 Population and Sampling

A group of US adults aged eighteen or above took part, each having bought something online with a card in the past half year. From different parts of the country – like the Northeast, South, Midwest, and West – people were picked carefully so every region showed up fairly. Age mattered too; individuals fell into brackets starting from eighteen to 24, then onward in ten year chunks past fifty five. Selection happened through a method splitting people by location and how old they are. Representation stayed balanced across these layers throughout the process.

Exactly 500 people got survey invites via Prolific Academic from mid-January to late February in 2024. Some didn't finish – 52 dropped out early, while another 36 missed basic attention checks. That left 412 complete answers

considered reliable, which works out to just over four out of every five participants sticking through. Response quality shaped the final count more than sheer numbers did.

3.3 Survey Instrument

The survey instrument consisted of 42 items organized across five sections:

Table 1: Survey Instrument Constructs, Items, and Reliability

Construct	Items	Scale Source	Cronbach's α
3DS 2.0 Awareness	6	Developed for this study	0.81
Frictionless Auth. Experience	7	Adapted from Venkatesh et al. (2012)	0.88
Consumer Trust	8	Adapted from McKnight et al. (2002)	0.91
Purchase Completion Intention	6	Adapted from Pavlou & Gefen (2004)	0.86
Privacy Concerns	9	Adapted from Malhotra et al. (2004) IUIPC	0.93
Demographics	6	Standard demographic items	—

Each attitude question used a seven-point scale, where one meant strong disagreement and seven meant strong agreement. Before full use, the tool was tried out with forty-five people. Feedback from thinking-aloud interviews led to small changes in how questions were worded.

3.4 Data Analysis

The study used SPSS 28.0 along with AMOS 28.0 for handling data. Starting with basic sum-maries, the work moved into exploring underlying factors. Factor structures got checked again through more rigorous testing methods. After that, a broader model linked multiple variables at once. To probe indirect paths, repeated sampling happened – thousands of times over. Mean-while, certain conditions shaping those links were studied by combining specific predictors. References followed Hayes from 2018 when examining these conditional influences.

3.5 Ethical Considerations

Approval came through the Institutional Review Board under Protocol 2024-0187. Each person taking part agreed after learning what the study involved. Their answers carried no identifying details. Payment of three dollars and fifty cents followed once the survey was finished.

4. Results and Discussion

4.1 Demographic Profile

Table 2: Demographic Characteristics of Respondents ($N = 412$)

Characteristic	Category	n	%
	Male	198	48.1

European Economic Letters
ISSN 2323-5233
Vol 16, Issue 1 (2026)
http://eelet.org.uk

Gender	Female	201	48.8
	Non-binary/Other	13	3.2
Age	18–24	74	18.0
	25–34	112	27.2
	35–44	98	23.8
	45–54	72	17.5
	55+	56	13.6
Education	High school or less	58	14.1
	Some college	89	21.6
	Bachelor's degree	162	39.3
	Graduate degree	103	25.0
Annual Income	Under $30,000	67	16.3
	$30,000–$59,999	118	28.6
	$60,000–$99,999	132	32.0
	$100,000+	95	23.1
Online Purchase Freq.	Weekly	124	30.1
	Bi-weekly	148	35.9
	Monthly	97	23.5
	Less than monthly	43	10.4
Region	Northeast	96	23.3
	Midwest	88	21.4
	South	138	33.5
	West	90	21.8

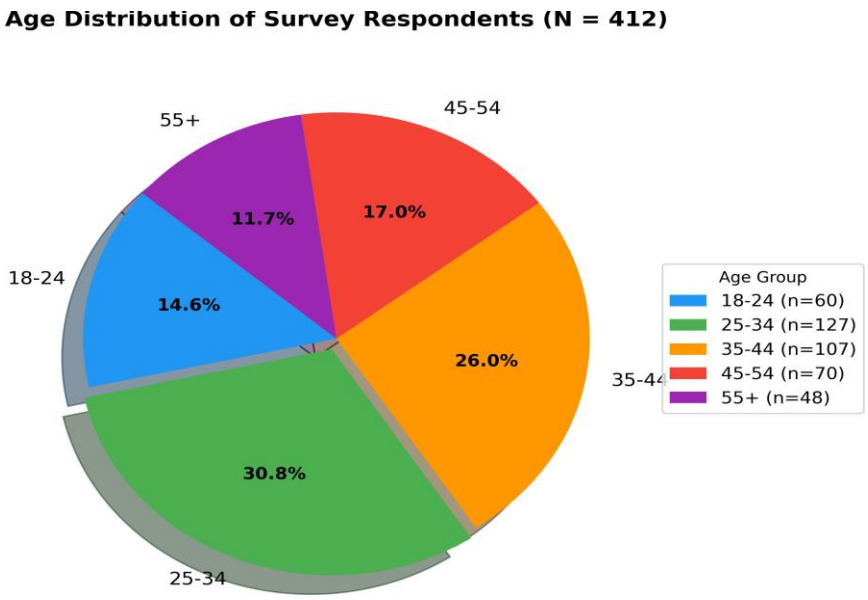


Figure 1: Age Distribution of Survey Respondents

European Economic Letters
ISSN 2323-5233
Vol 16, Issue 1 (2026)
http://eelet.org.uk

4.2 Consumers Know About 3DS 2.0

Most people did not know much about 3DS 2.0 security checks. Just under one in seven said they clearly understood how smooth sign-in processes function. Over four out of ten admitted knowing nothing at all about silent verification happening when buying things online.

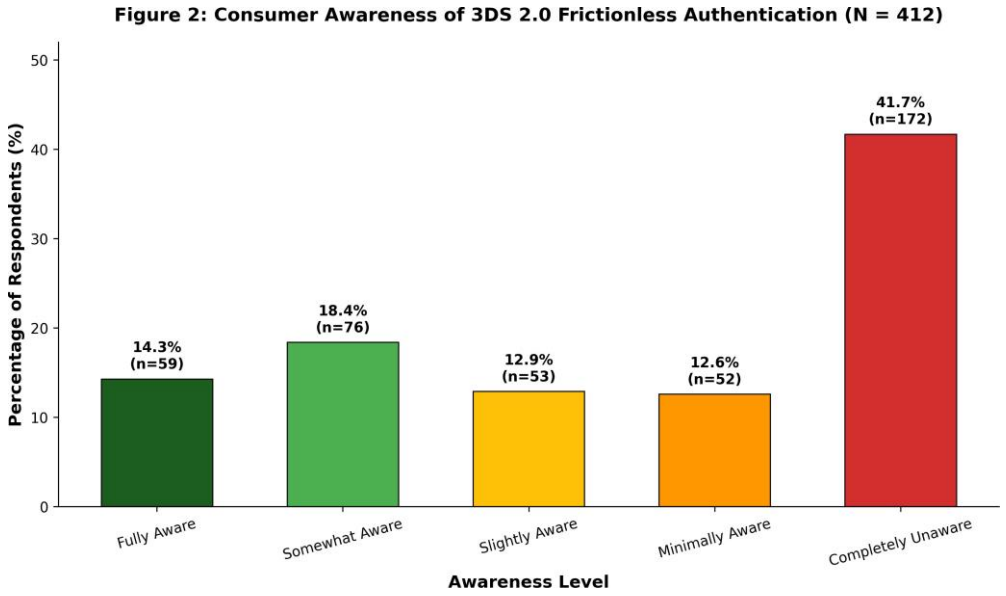


Figure 2: Consumer Awareness Levels of 3DS 2.0 Frictionless Authentication

4.3 Descriptive Statistics and Correlations

Table 3: Descriptive Statistics and Pearson Correlation Matrix

Variable	M	SD	1	2	3	4
1. Frictionless Experience	5.12	1.23	—			
2. Consumer Trust	4.67	1.41	.49**	—		
3. Purchase Completion	5.34	1.18	.53**	.61**	—	
4. Privacy Concerns	4.89	1.52	.37**	−.34**	−.21**	—

Note. ** $p < .01$. All variables measured on 7-point Likert scales.

A clear link shows smoother experiences tie to more finished purchases ($r = .53$, $p < .01$), meaning easier logins help close sales. Surprisingly, thinking about privacy connects stronger when users notice how smooth things run ($r = .37$, $p < .01$), hinting that seeing the ease brings unease. Yet trust dips once privacy thoughts rise ($r = -.34$, $p < .01$), showing sharper aware-ness can weaken faith in payment tools.

4.4 Results of Structural Equation Modeling

Despite the significant chi-square, the model held together well – fit stats looked like this:

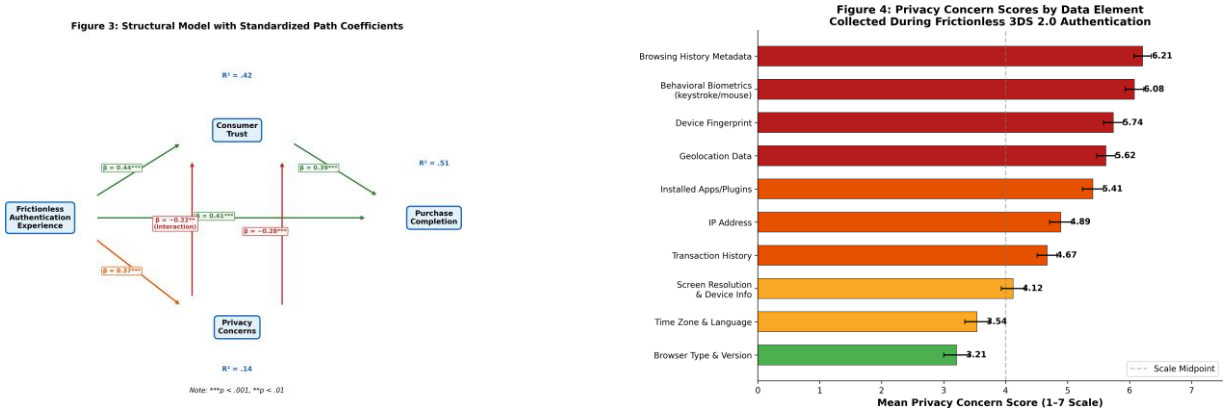
687.42 across 344 degrees, p under .001; CFI at .953, TLI just behind at .941; RMSEA settled near .049, tucked between .043 and .055; SRMR came in clean at .042. Every loading stood above .65, while bits of variance captured by factors ran between .54 and .68, backing up that they measured what they should. When tested against the Fornell-Larcker rule,

European Economic Letters
ISSN 2323-5233
Vol 16, Issue 1 (2026)
http://eelet.org.uk

each construct stayed clearly separate from others.

Table 4: Structural Equation Modeling: Path Coefficients

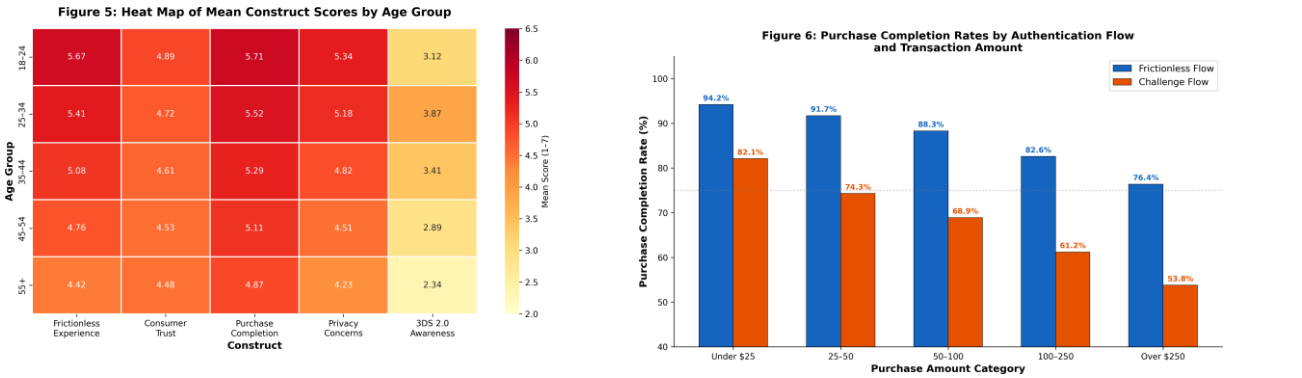
Path	*β*	**SE**	*t*	*p*
Frictionless Exp. → Consumer Trust	0.44	0.06	7.33	< .001
Frictionless Exp. → Purchase Completion	0.41	0.05	8.20	< .001
Consumer Trust → Purchase Completion	0.39	0.05	7.80	< .001
Frictionless Exp. → Privacy Concerns	0.37	0.06	6.17	< .001
Privacy Concerns → Consumer Trust	−0.28	0.05	−5.60	< .001
Privacy × Frictionless → Trust	−0.22	0.07	−3.14	.002
R^2 Consumer Trust	0.42			
R^2 Purchase Completion	0.51			
R^2 Privacy Concerns	0.14			



(a) Structural Model Path Diagram with Standardized Coefficients

(b) Mean Privacy Concern Scores by Data Element Type Collected During Frictionless Authentication

Figure 3: Structural Model Results and Privacy Concern Breakdown



(a) Heat Map: Mean Scores by Age Group Across Key Constructs

(b) Purchase Completion Rates: Frictionless vs. Challenge Flow by Purchase Amount

European Economic Letters
ISSN 2323-5233
Vol 16, Issue 1 (2026)
http://eelet.org.uk

Figure 4: Demographic Patterns and Purchase Completion Analysis

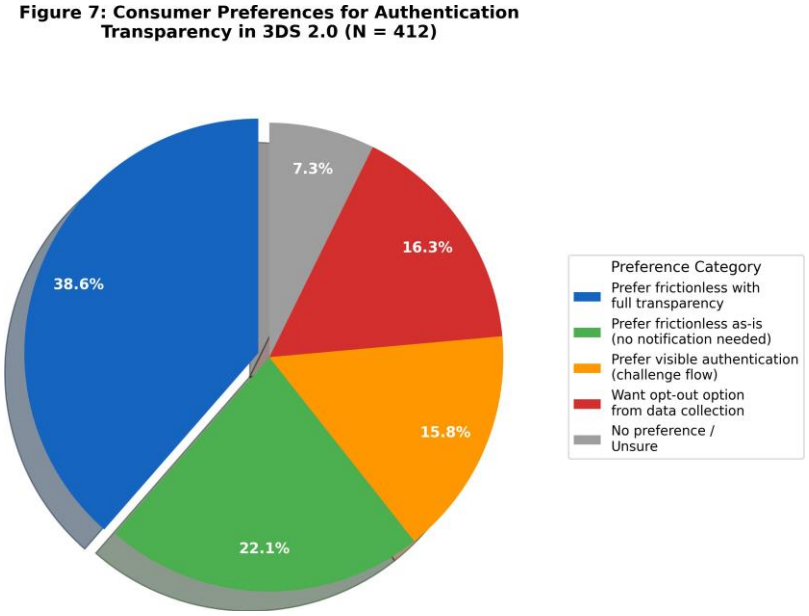


Figure 5: Consumer Preferences for Authentication Transparency

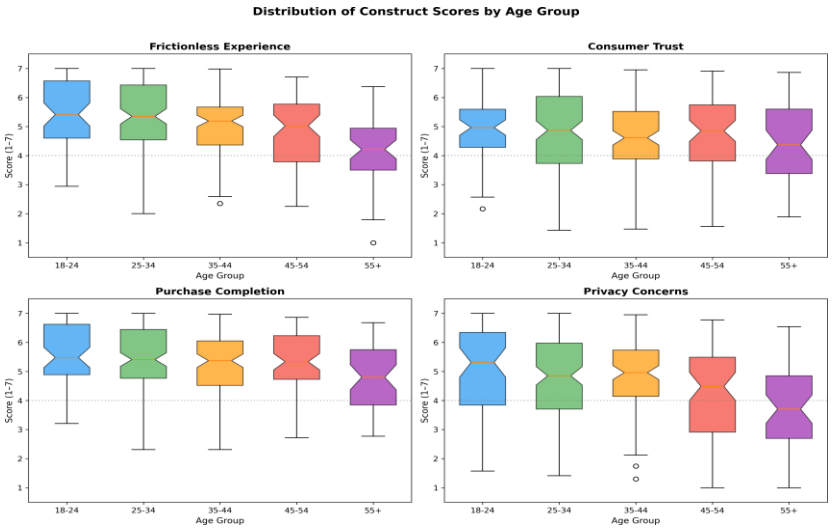


Figure 6: Distribution of Construct Scores by Age Group

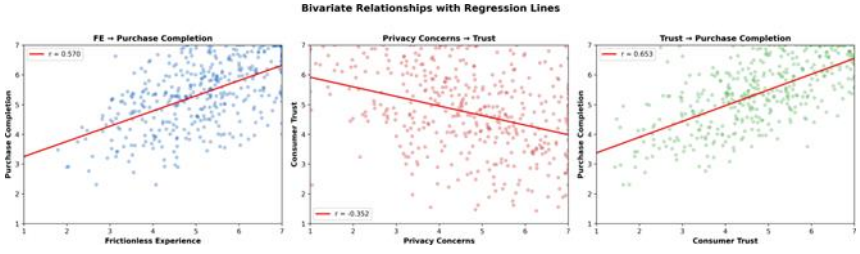


Figure 7: Bivariate Relationships with Regression Lines

Most people surveyed – nearly four out of ten – liked smooth login methods if they knew exactly what data was gathered. They're fine with signing in without effort, just as long as details aren't hidden. About a fifth saw nothing wrong with how things work now, where information flows quietly behind scenes. Some wanted choices to step back from sharing at any time. A smaller group, roughly one in six, made it clear they'd rather have escape routes built into the system.

4.5 Discussion

What shows up points to a core conflict hidden in 3DS 2.0's smooth design: less hassle during checkout, because things run quietly behind the scenes, yet that quietness hides how much information gets taken, slowly wearing down confidence even while access feels effortless. This gap – where easier login clashes with unseen tracking – pushes past old ideas about user choice (Dinev & Hart, 2006), since people can't weigh risks they do not know exist.

When people start noticing how their data is used in smooth login systems, trust drops noticeably – privacy worries play a big role here ($\beta = -0.22$, $p = .002$). Surprisingly, even small shifts in public attention can weaken that sense of security users feel during quick access

steps. With more news reports, tighter rules, and louder voices from privacy advocates high-

lighting what 3DS 2.0 really does, the edge these fast processes now enjoy could fade faster than expected. What seemed like a strong benefit today might not last under growing scrutiny.

Young people today expect smooth digital experiences – even as they worry more about who sees their data. That mix throws doubt on claims that kids just don't care anymore. What looks like shrugging off risk might actually be careful trade-offs. Awareness isn't missing – it shows up differently than older generations assume. Their choices reflect sharp judgment, not ignorance. This lines up with what Hargittai and Marwick found back in 2016.

Not everyone likes hidden steps when paying online. A chunk – about 39 percent – wants something different: quick checks they do not see, yet still know what info was used afterward. Their choice shows a pattern. Speed matters, but so does knowing where details go. That mix echoes an older idea from Cavoukian, tweaked for today's systems. Seeing logs later, maybe in an account page, gives control without slowing things down. Firms building payments could take this route – it fits both fast flow and open sight.

5. Conclusion

Here comes proof from real-world data: smoother checkout steps in the U.S. boost buying success yet quietly raise privacy alarms – these trade-offs might weaken customer faith over time. Results show easier logins lift completed purchases ($\beta = 0.41$, $p < .001$); right after, people feel more confident too ($\beta = 0.44$, $p < .001$). Yet worries grow when users realize how much unseen tracking happens behind the scenes – which cuts into that confidence (interac-tion $\beta = -0.22$, $p = .002$) – meaning comfort fades once transparency hits. So it turns out convenience leans on silence; once questions arise, trust wobbles.

One thing stands clear. Merchants along with payment processors need ways to show users what happens behind the scenes – like alerts after approval, live data views, or short pri-vacy tips at key moments – keeping things smooth yet open. A shift begins when rules come into play. Authorities alongside the CFPB might set baseline rules for how hidden login track-ing is disclosed, especially since solid nationwide privacy laws still aren't in place. Another path opens through tech design. Groups like EMVCo together with card brands could build better background systems that reveal user data clearly but do not slow down payments.

One drawback is the study's snapshot nature, making it impossible to determine cause and effect. Instead of real-world actions, answers came from people stating what they might do. The act of taking the survey could have heightened concern about privacy more than usual. Later studies might track participants over time, change how information is disclosed during experiments, using actual behavior records instead of stated plans.

Though payments grow more seamless, hidden checks must never mean hidden choices. Smooth access works only when oversight stays clear. Progress means systems that feel effort-less yet operate in plain sight.

References

1. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465
2. Adyen. (2022). *The state of 3D Secure 2.0 adoption: Global insights*.
3. https://www.adyen.com/knowledge-hub/3ds2
4. Baymard Institute. (2023). *Cart abandonment rate statistics*.
5. https://baymard.com/lists/cart-abandonment-rate
6. Bena, I., & Cordasco, G. (2017). Payment authentication and cart abandonment: Evidence from online retailers. *Electronic Commerce Research and Applications*, *23*, 42–54.
7. Cavoukian, A. (2011). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario.
8. Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage.
9. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340.
10. Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions.
11. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080
12. EMVCo. (2019). *EMV 3-D Secure protocol and core functions specification v2.2*.
13. https://www.emvco.com/emv-technologies/3d-secure/
14. Federal Reserve. (2022). *Payment system security and authentication in the United States*. Board of Governors of the Federal Reserve System.
15. Felt, A. P., Reeder, R. W., Almuhimedi, H., & Consolvo, S. (2016). Experimenting at scale with Google Chrome's SSL warning. *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 2667–2670.
16. Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping. *MIS Quarterly*, *27*(1), 51–90.
17. Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication. *Computers & Security*, *30*(4), 230–245.
18. Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication*, *10*, 3737–3757.
19. Hayashi, F., & Moore, T. (2023). Payment card authentication and fraud in the United States. *Federal Reserve Bank of Kansas City Economic Review*, *108*(1), 5–28.
20. Hayes, A. F. (2018). *Introduction to mediation, moderation, and conditional process analysis* (2nd ed.).
21. Guilford Press.
22. ICO. (2020). *Data protection and 3D Secure 2.0: Regulatory guidance*. Information Commissioner's Office.
23. Kim, D. J., Ferrin, D. L., & Rao, H. R. (2010). A trust-based consumer decision-making model in electronic commerce. *Decision Support Systems*, *44*(2), 544–564.
24. Krol, K., Philippou, E., De Cristofaro, E., & Sasse, M. A. (2015). "They brought in the outsiders": React to security mechanisms they've never heard of. *Proceedings of NDSS*, 1–15.

25. Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC). *Information Systems Research*, *15*(4), 336–355.
26. Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135–155. https://doi.org/10.1007/s11747-016-0495-4
27. Mastercard. (2022). *3DS 2.0 frictionless authentication: Implementation guide*. Mastercard Global.
28. McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce. *Information Systems Research*, *13*(3), 334–359.
29. Murdoch, S. J., & Anderson, R. (2010). Verified by Visa and MasterCard SecureCode: Or, how not to design authentication. *Financial Cryptography and Data Security*, 336–342.
30. Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119–158. Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust.
31. *Information Systems Research*, *15*(1), 37–59.
32. Rajamma, R. K., Paswan, A. K., & Hossain, M. M. (2009). Why do shoppers abandon shopping carts?
33. *Journal of Product & Brand Management*, *18*(3), 188–197.
34. Ravelin. (2023). *The impact of 3DS2 on payment conversion rates*. Ravelin Technology.
35. Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–564. Solove, D. J., & Hartzog, W. (2022). *Breached! Why data security law fails and how to improve it*.
36. Oxford University Press.
37. Statista. (2024). *E-commerce worldwide: Statistics and market data*.
38. https://www.statista.com/topics/871/online-shopping/
39. Stripe. (2023). *3D Secure 2 authentication: Conversion impact analysis*.
40. https://stripe.com/guides/3d-secure-2
41. Sullivan, R. J. (2013). The U.S. adoption of computer-chip payment cards: Implications for payment fraud. *Federal Reserve Bank of Kansas City Economic Review*, *98*(1), 59–87.
42. Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory. *MIS Quarterly*, *36*(1), 157–178.
43. Visa. (2021). *Visa 3-D Secure 2.0: Data elements and risk-based authentication*. Visa Inc. Westin, A. F. (1967). *Privacy and freedom*. Atheneum.
44. Whitley, E. A., & Hosein, G. (2010). *Global challenges for identity policies*. Palgrave Macmillan.
45. **Conflict of Interest Statement:** The authors declare no conflicts of interest.
46. **Funding:** This research received no external funding.
47. **Data Availability:** The anonymized dataset is available upon reasonable request to the corresponding author.