LOGIN.GOV

Observational Study Synthesis

Author: Alexander Hoover

Session moderators: Carrie McGrath - QQ2C Shqiponja Hoxha Ocumarez - QQ2-C Princess Ojiaku - QUEACB Annie Hirshman - QQ2C Kelli-Anne Ho - QQ2-C Alexander Hoover

Session notetakers: Thomas Emerick - QQ2-C Shqiponja Hoxha Ocumarez - QQ2-C Alexander Hoover Carrie McGrath - QQ2C Chanan Delivuk - QQ2C Annie Hirshman - QQ2C Kelli-Anne Ho - QQ2-C Travis Newby Leanna Miller Elizabeth Manning

Special thanks to: John Rahaghi (VA), Amanda Porter (VA), Crystal Dugan (Perigean), Josh Kim (Ad Hoc via VA), Angela Fowler (Ad Hoc via VA), David Kennedy (Ad Hoc via VA), Alyssa Gallion (VA), Andrea Hewitt(Oddball via VA), Shane Strassberg (VA), Rutvika Gupta - QQ2-C , Benjamin Chait - QQ2D , Jessica Dembe - QD1D-C

Summary

- A little under half (10 of 21 sessions) of the participants successfully created an account and proved their identity.
    - Of the other 11 participants,
        - 9 abandoned, were rate limited, or were blocked, and
        - 2 encountered staging bugs or ran out of time.
        - The biggest issues frustrating or blocking people from completing the process were related to photo ID upload.
- 14 of 21 participants chose one MFA option.
    - SMS and Face/Touch were basically the only options people picked, with backup codes being a distant third (and never the first option).
    - Most participants selected one MFA for convenience.
    - Some participants seemed to believe having more MFA options was about improving security and felt their one MFA was secure enough.
- Login.gov is not usable for screenreader participants.
    - 3 of the 5 screenreader participants were unsuccessful for reasons related to their being dependent on a screenreader.
    - 2 of those participants were blocked at the photo ID upload step.
    - One participant was blocked earlier because they had trouble navigating the sign-in page.
- Users do not have fallback options to verify personal details or phone number.
    - 3 of 21 participants said they did not know how to proceed when rate limited or blocked by a failure to verify something.
- Difficulty with a Puerto Rican address
    - The one participant with a PR address was rate limited after submitting their address for verification too many times.
    - We can see this issue with Puerto Rico in the data. The InstantVerify success rate for Puerto Rico is 12.46%. The InstantVerify rate for all Login.gov users is 82.03%.
- No state-issued photo ID
    - 2 participants did not have a state-issued ID. One had an NYC municipal ID. The other had a DoD-issued ID. Both abandoned at photo ID upload.

About the study

The goal

Get a baseline understanding of how users experience Login.gov's unsupervised proofing flow, including challenges they face and how they seek to overcome them.[1]

The context

Before this study, the only observational study of users' experience with Login.gov focused on users with low/no vision. Login.gov researchers have proposed studies of a broader user base in the past. This team was able to make this study happen by partnering with VA, who provided participant recruitment and compensation.

The sessions

The study consisted of 21 remote, hour-long sessions between 10/14 and 12/5/2022. In addition to the participant, a facilitator, and a notetaker, we had some observers from Login.gov and VA join. Accessibility specialists from VA joined as needed.

Who we talked to

We talked to 21 participants. 3 came from a USDS-recruited trial run. The remaining 18 were veterans recruited through the VA. Our participants included:[2]

- 5 who were regular users of assistive technology, like screenreaders.
- Even split of 8 men and 8 women. 2 participants identified as non-binary.
- 7 participants reported income less than 40k
- At 8 participants, "Black or African American" was the largest racial/ethnic group in the study.

[1] Full research plan at: Direct Observation Study: Understanding Challenges with Unsupervised ...
[2] Full breakdown of the study's demographics is available in Participant Tracker + Analysis

Some numbers

Results of the sessions

A little under half (10 of 21 sessions) of the participants successfully created an account and proved their identity. We had two sessions that ended early because of a staging.login.gov bug or we ran out of time. The remaining 9 sessions (of 21) were Rate Limited, Blocked, or Abandoned.

Table 1. Count and rates of each possible session result.

Result	Count	Percentage	Definition
Success	5	24%	Participant successfully created account and verified ID without any errors or issues.
Success with bumps	5	24%	Participant successfully created account and verified ID but encountered some errors or issues (e.g., had to upload photo ID more than once).
Abandoned	4	19%	Participant gave up or said they would give up in real life.
Blocked	3	14%	A close cousin of "Abandoned" and “Rate Limited.” Participant was blocked at a step but did not hit the rate limit and sought customer support help.
Rate Limited	2	10%	Participant received message saying that they attempted a step too many times and must wait X hours to try again.
Bug	1	5%	Login.gov staging had a bug that prevented the participant from going through the full flow.
Incomplete	1	5%	Time was up before the participant could complete the full account creation and identity proofing flow.

Reasons for Abandoned, Blocked, Rate Limited, or Success with Bumps

Most participants that had an issue with Login.gov had an issue at the “Upload state photo ID” step. Most participants were able to succeed despite these issues.[3] Some were blocked or abandoned. Other participants abandoned or were blocked for reasons related to Login.gov’s accessibility or gaps in data.

Table 2. Analysis of each participant that abandoned, was blocked, was rate limited, or had success with bumps.

Participant	Result	Step Where Issue(s) Occurred	Issue Theme
2	Success with bumps	11 - [Phone] Upload state photo ID	Uploaded wrong photo of photo ID
4	Success with bumps	11 - [Phone] Upload state photo ID	Auto-capture produced blurry photo
8	Success with bumps	11 - [Phone] Upload state photo ID	Auto-capture too sensitive
11	Success with bumps	11 - [Phone] Upload state photo ID	Auto-capture produced blurry photo
12	Success with bumps	11 - [Phone] Upload state photo ID	Manual upload. Unclear to participant what the problem was with the photo.
3	Rate limited	11 - [Phone] Upload state photo ID 15 - "Verify your information"	Bump - light background for uploaded photo Rate limited - PR address, not clear which variation is correct
17	Rate limited	11 - [Phone] Upload state photo ID	Auto-capture produced blurry photo Manual upload. Unclear to participant what the problem was with the photo.

[3] The number of participants that had “success with bumps” should probably be discounted a bit. We should assume that at least a few of these folks would have abandoned and maybe come back later. Participants in a study will often proceed with a study for the study’s sake.

14	Blocked	16 - “Enter a phone number with your name on the plan”	Could not verify phone number
15	Blocked	16 - “Enter a phone number with your name on the plan”	Could not verify phone number
18	Blocked	11 - [Phone] Upload state photo ID	No state-issued photo ID
6	Abandoned	11 - [Phone] Upload state photo ID	Not comfortable uploading ID
10	Abandoned	1 - Sign-in	Could not find "Create an account" button
13	Abandoned	11 - [Phone] Upload state photo ID	Manual upload. Unclear to participant what the problem was with the photo.
16	Abandoned	11 - [Phone] Upload state photo ID	Could not use auto-capture

See Participant Tracker + Analysis for more detailed description of issues.

Multi-factor authentication

14 of 21 participants chose one MFA option. SMS and Face/Touch were basically the only options people picked, with backup codes being a distant third (and never the first option). Nobody had a security key. None of the participants had a PIV. People either didn't know what an authenticator app was or they knew what it was but didn't want another app on their phone.

Table 3. Breakdown of participant choices for multi-factor authentication.

MFA Combos	Count	Percentage
SMS + Skip	10	48%
SMS + Backup codes	3	14%
Face/touch + SMS	3	14%
Face/touch + Skip	3	14%
NA + NA	1	5%
Voice + Skip	1	5%

Product-level issues

During the study, the team saw a variety of participant experiences. Some participants sailed through without issue. Others abandoned out of frustration or were blocked. For the issues that blocked or caused abandonment, Login.gov will need more than UI/content refinements. These issues include:

- Photo upload was difficult for many
- Login.gov is not usable for screenreader participants
- No fallback options to verify personal details or phone number
- Difficulty with a Puerto Rico address
- No state-issued photo ID

Addressing these issues will require rethinking Login's flow, coming up with new interactions, and new procurements.

Issues

Photo upload was difficult for many

11 of 21 participants struggled at the photo ID upload stage. Some participants were able to make it through in spite of the struggles. Others were blocked or abandoned. Participant struggles with photo ID upload largely stemmed from the rigidity of the technology used to upload and analyze an ID. Either auto-capture proved cumbersome or participants had trouble getting manual pictures just right for successful analysis.

Difficulty with auto-capture

5 of the 21 study participants had an issue with auto-capture on a mobile device. The issues were not always blocking but did create a less-than-smooth experience. The difficulties fell into one of three groups:

- Auto-capture was too sensitive.

- Auto-capture took a picture and then said it was too blurry.
- Auto-capture inaccessible to screenreader users.

Where auto-capture was too sensitive for participants, they had trouble lining up their ID with the four corners provided by auto-capture on their phone. P8 captured it succinctly when they said, "That's a little sensitive...goes directly from move closer to too close."

Where the auto-captured photo was too blurry, participants had to try multiple times to get the photo right. The flow was generally that the participant would line up their ID in the four corners, get the 3-2-1 counter, the auto-capture tool would take the photo, and then the participant would get a "too blurry" error back on the page showing where to upload front and back photos of the ID. Many times, the participant had no idea why their first attempt failed:

> Just want to take the damn photo... I'm busy!...[Took another photo and it worked.]... I had to try twice, but I have no idea why because I didn't do anything different than the first time. Maybe I was a little shaky so it was a little bit blurry? - p12

Auto-capture was generally inaccessible for participants using screenreaders. These issues are discussed more in Login.gov not usable for screenreader participants.

Difficulty with manual upload

5 of the 21 study participants had an issue with manually taking and uploading photos. These participants struggled to meet all the requirements for a successful manual upload (e.g., dark background, ID is 80% of the photo, etc). Participants generally did not read the guidance on the page, opting to just jump into upload photos.

The root cause is that the photos looked good to the participants[4], even if they weren't what Login needed. Participants could see the ID clearly but the automation on the backend could not.

Login.gov is not usable for screenreader participants

3 of the 6 screenreader participants were unsuccessful for reasons related to their being dependent on a screenreader. One screenreader participant (p14) was able to make it to the "Verify phone or address" step, but the session ran out of time. That participant did have some vision, relying primarily on magnification and a little on their screenreader.[5] These findings are consistent with findings from VPAT Blind and/or Low-Vision Disability Testing Report 2022.

Listen to a clip of a participant trying to use the photo ID auto-capture.

Table 4. Result and session description of each screenreader participant.

Participant	Result	Result Description
10	Abandoned	Did not get beyond the sign-in screen. Assistive tech user.
14	Blocked	Phone number not verified with Phone Finder. Issues with photo ID upload.
16	Abandoned	Assistive tech user. Unable to get beyond the auto-capture ID upload.
17	Rate limited	Rate limited on upload photo ID. Assistive tech user.
20	Incomplete	Ran out of time. Stopped at Phone Finder.
21	Bug	Issue with staging. Bug that prevented state id upload from desktop. Did not even try to upload from phone. Only wanted to upload from desktop.

[4] "Picture that I sent is readable on my screen" - p8

[5] We did not capture the level of vision in our screener survey. We only asked if the participants used a screenreader. Although not explicitly asked, we believe the 3 participants that were unsuccessful were either blind or nearly blind and much more reliant on the screenreader.

No fallback options to verify personal details or phone number

"I don't know what else to try." - p14

3 of 21 participants said they did not know how to proceed when rate limited or blocked by a failure to verify something. In each of these cases, Login failed to verify the participant's address or phone number. Only one participant (p14) eventually found the verify-by-mail option below the fold and said they'd pursue that option or try to call customer support.

The solutions participants offered up to continue the verification process often amounted to playing a guessing game.

> In 6 hours, I could try again, but I don't know what I'd do differently. I will keep trying different ways of entering my address. - p3 [6]

One participant called out that the rate-limited delay in some contexts could be a significant problem, stating "6 hours in an emergency is a long time."[7]

Difficulty with a Puerto Rican address

One participant (p3) lived in Puerto Rico. They were ultimately rate limited because they tried to submit their Puerto Rican address for verification too many times.[8] Systems commonly have trouble verifying addresses from Puerto Rico.[9]

[6] This was a person familiar with the inner workings of Login and knew about issues with PR addresses. Had the participant not had this knowledge of Login, it is unclear how they would have proceeded.

[7] Participant 3

[8] Complicating this participant's experience is that the address on their ID was not the same address they use when getting deliveries. They lived close to the border of another town and often had to put their address as being in the other town to get packages delivered. This nuance made it less clear which address the participant should use.

[9] "In some parts of Puerto Rico, it's not uncommon to have multiple addresses with the same street name and same house number in the same ZIP Code. Some rural areas don't even have formal addresses for housing units." See, "Street Addresses Are Simple, Right? Not in Puerto Rico", Census.gov, https://www.census.gov/library/stories/2020/01/street-addresses-are-simple-not-in-puerto-rico.html (last visited Dec. 13, 2022)

This participant's experience was not a one-off occurrence. We can see this issue with InstantVerify and Puerto Rico in the data. The InstantVerify success rate for Puerto Rico is 12.46%.[10] The InstantVerify rate for all Login.gov users is 82.03%. That's a ~70% gap. The data maintained for Puerto Rico by InstantVerify is clearly lacking.

Complicating this problem further, Puerto Rico has one of the highest proofing attempt rates of any state or territory. 0.10% of the Puerto Rican population attempted identity proofing with Login.gov between Oct. 25 and Nov. 1, 2022.[11] This is second only to Florida, with 0.12%.[12] Other states and territories have proofing attempt rates between 0.01% and 0.06% of their population. There is a clear demand for Login.gov in Puerto Rico that Login.gov is not meeting because of issues with InstantVerify.

No state-issued photo ID

"I'm kinda stuck if I don't have a state ID." - p18

2 participants tried to use photo IDs that were not state-issued. One participant (p18) had an NYC municipal ID and no state-issued photo ID. They are a disabled vet that uses VA benefits and services. They were unable to proceed past the "Upload photo ID" step. The participant said that they did not want to go to the post office because their disability made travel difficult. In-Person Proofing would not have helped at this time, as only state-issued IDs are accepted.

Another participant (p6) had an ID issued by the Department of Defense. They were confused why they couldn't use a DoD ID to verify their identity with the VA. The session prompt had participants imagining they were trying to create a Login.gov account to get into the VA's site to access information or benefits. The participant ultimately abandoned because they did not want to try uploading another ID.

[10] For Oct. 25 - Nov. 1, 2022. See Identity Transaction Results – Oct 25 - Nov 1, 2022

[11] Identity Transaction Results – Oct 25 - Nov 1, 2022

[12] Identity Transaction Results – Oct 25 - Nov 1, 2022

Research from a previous discovery sprint suggests that as much as 11% of U.S. citizens do not have a government issued photo ID. That rate is significantly higher for some specific groups (e.g., 25% of African-Americans do not have a government issued photo ID).[13]

[13] Possession of ID Documents, Remote Identity Proofing with Supervision Contingency Sprint Report (October 2022) (citing "Citizens without Proof: A survey of Americans' possession of documentary proof of citizenship and photo identification", Brennan Center for Justice, https://www.brennancenter.org/sites/default/files/legacy/d/download_file_39242.pdf (last visited Dec 16, 2022)

Possible next steps

Below are some recommendations on how Login.gov can address the product-level issues.

Explore better auto-capture solutions

A Login.gov team of designers, engineers, product, procurement, and accessibility specialists should find an auto-capture UI pattern that is more forgiving. The current auto-capture pattern caused usability issues for some, was a blocker for others, and presents a serious equity issue for Login.gov. A more forgiving pattern could help users pass ID verification and increase overall success rates.

As an example of what a new pattern might look like, both Evernote and Apple Notes have document scanning patterns that require a lot less manual alignment from the user (watch an example of Apple Notes document scan). The scanner does the work of finding and properly capturing the document. A pattern like that might reduce the number of issues users have with Login's photo ID auto-capture.

Some other ideas to explore as part of this work include:

- Auto-detect the front and back of an ID, making photo ID upload possible for users who are blind and just a little easier for other users.
- Allow upload with a desktop webcam.[14]

Any exploration would need to take into account a possible solution's usability with assistive technology, like screenreaders.

Shifting the burden of taking a good picture onto technology and not the user could help users pass the ID verification step and increase overall success rates.

[14] 2 participants (p2 and p13) wanted an option to use their desktop webcam to take a picture of their photo ID.One participant (p13) commented, “I've seen other sites where you can use your webcam. I think it's the doctor's office. That's a whole lot easier than what I'm trying to do now." That same participant ended up abandoning the process because they had trouble upload their ID through their phone.

Remote identity proofing with supervision

Remote identity proofing with supervision (RIPS), and the flexibility it offers, could help blocked users at the address or phone verification steps and improve accessibility.

RIPS could give users a path to success when they're blocked at InstantVerify or PhoneFinder (see No fallback options to verify personal details or phone number). This was specifically discussed in the RIPS Fair Evidence Pilot recommended in Remote Identity Proofing with Supervision Contingency Sprint Report. By allowing other pieces of fair evidence, RIPS would allow users not covered by current LexisNexis databases to verify their identity in a NIST-compliant way.

Although not originally envisioned in the RIPS Contingency Sprint Report, RIPS could also help improve accessibility for participants using a screenreader. Some of the issues participants using screenreaders encountered included not being able to tell which side of their ID was the front or back and inability to use the auto-capture feature with a screenreader to properly align their ID. Login.gov could explore if a video chat agent could address these issues by allowing users to share documents over a webcam.

The accessibility issues we observed in this study should inform possible RIPS implementations. The RIPS Fair Evidence Pilot originally imagined users uploading other pieces of fair evidence (e.g., utility bills, W2s) similar to how users upload their photo IDs now. Given the usability and accessibility issues with the current photo ID upload process, a RIPS pilot should look at other methods of document upload (e.g., Explore better auto-capture solutions).

Human in the loop

Human-in-the-loop (HITL) could also play a role in addressing issues with photo uploads and some of the accessibility issues discussed above. HITL could make the photo ID upload process more usable and accessible by allowing for more flexibility in the quality of photos uploaded.

Many of the usability and accessibility issues participants encountered in their sessions stemmed from the rigidity of the requirements for a good photo. There was a clear disconnect between what was a “good photo” to the participant (“Looks good to me”) and what was a “good photo” to LexisNexis/Acuant. Many participants that had issues with manual upload took photos that were perfectly legible to a human but did not have a dark background or the ID did not occupy a big enough portion of the picture.

We recommend testing the hypothesis that a human in the loop reviewing these pictures very likely could use these “bad” photos to collect the necessary information and check for security features. The pictures were often clear to the participant and even the session facilitator viewing the pictures over Zoom.

Login.gov has looked into HITL before.[15] The strategy at the time was to see what Login could do with existing vendor. An initial conversation with an existing vendor that offers some HITL services did not go very well. If Login decides to pursue a HITL strategy, Login should clearly define HITL requirements it wants to see from the market by conducting market research, writing up an RFI, and putting out a call for proposals. HITL is a known strategy in automation.[16] The market should have more to offer.

Define personas for Login.gov users

Login.gov should define its own personas to help guide future research and the product roadmap.[17] Many of the issues discussed so far are a result of groups not being accounted for in the data or UI development. Personas can help Login.gov

[15] 1-pager: HITL as a test

[16] Example from Uber: https://eng.uber.com/ubers-real-time-document-check/. Example from Google: https://cloud.google.com/document-ai/docs/hitl

[17] Although not fully developed personas, the recent RFI that Login put out specifically raised the issue of how vendors will serve groups that have been traditionally left out of ID proofing solutions. Draft RFI 11.22.22

better understand who is and is not served by the product. In this study alone, the team observed participants from 3 groups that are not well served by Login.gov:

- Blind or low-vision users
- Users living in Puerto Rico and other U.S. Territories
- People without a state-issued photo ID

These participants were blocked by accessibility issues, data quality issues, or gaps in the kinds of ID Login.gov recognizes. Each of these blockers and the impact on specific groups present serious equity issues for Login.gov.

Clear personas could help Login.gov gain a more nuanced understanding of the issues facing the product and offer a focused course of action. Personas combined with the recent work on OKRs could be very powerful. For example,

- What is the current impact of Login.gov's inaccessibility for blind/low-vision users on Login.gov's success rate? How does this vary across partner agencies? How might improvements for those users help meet that 5% success rate increase OKR?
- How do the address verification issues for users living in Puerto Rico affect success rates for Login.gov at SBA and generally?

Login.gov does not necessarily need to set out to define every single persona using the product right now. Work can start on expanding on the 3 groups discussed here, to the extent necessary. The life experiences described in the recent Customer Experience Executive Order are a good place to look next. Those life experiences were picked specifically because they require interaction with several government agencies. Login.gov plays a very clear role in making those agency interactions as seamless as possible.

By taking small, iterative steps to define Login.gov's personas, the team can work towards a more nuanced understanding of the issues facing the product and how to address those issues.[18]

[18] This work has been started and should continue with the support of Login.gov leadership. See, Login Populations, Users, Personas

Issues requiring some UX love

The issues and opportunities described below are arguably not product-level concerns that require new tools and procurements. These are items that presented relative minor issues for participants or were interesting opportunities that came up in conversations with participants and the team.

Authentication issues

Multi-Factor Authentication

14 of 21 participants chose one MFA option.[19] The main reasons for skipping the second MFA option were something like "one should be enough" or "I'll do it later". If they weren't just saying it for the session, it could be interesting to see what we can do to make the "i'll do it later" folks actually do it later. We also heard 3 participants say that their first choice "was secure enough." This suggests a perception that having more options makes an account more secure.

"People will use the easiest one, to get the same info you are trying to get" - p11

Recommendations

- Follow up on the "I'll do it later" and "One is secure enough" users. How might Login actually get users to add another MFA later? Some ideas discussed by the team:
    - Follow-up email soon after account creation prompting them to add another MFA
    - A complete-your-profile pattern like on LinkedIn
    - A prompt in the account creation flow that comes at the end of account creation and identity verification

[19] Table 3. Breakdown of participant choices for multi-factor authentication.

- Prioritize making face/touch work. There are known issues with using face/touch on Login.gov. However, Apple and Google are working to address many of those issues, with clearly stated timelines. The technology is evolving. Given that face/touch was a fairly popular choice (6 of 21 participants) and was in the mix for 3 participants that chose 2 MFA options, Login.gov should explore how to adjust the face/touch implementation to take advantage of the changes to the technology. For example, can face/touch only be available for users that have iOS 16?[20]
- Explore content changes related to authenticator apps. Would including the names of specific authenticators make this a more popular option? A few participants were familiar with authenticator apps because of work. Would name dropping Duo or Google Authenticator make this a more familiar and viable option?

Confusion on how to fix a so-so password

6 of 21 participants had some non-blocking issues creating a strong enough password to proceed. At least 2 participants entered passwords that were less than 12 characters long. The guidance under the "so-so" label did not tell the participant that they didn't have enough characters. That guidance seemed to only offer guidance on creating a strong password (e.g., " common names and surnames are easy to guess") and did not speak to the password requirements listed above the password field.

When participants did go to improve their password so that they could continue, the passwords they created were often hard to remember. One participant (p2) commented, "Oh see, it liked it. It's not one I would use ever again, so I'm going to write it down."

The team acknowledges that the final outcome – participants creating strong passwords that they're unlikely to use elsewhere – is likely a desired outcome from

[20] Updates in iOS 16 let face/touch information to carry over to other Apple devices through iCloud. Still a lot to figure out there but worth some investigation.

a security perspective. And, these requirements did not end up blocking anyone. However, the experience getting there could have been a little smoother.

Recommendations and questions

- Update password strength guidance to include hard password requirements (e.g., “Your password must be at least 12 characters”). Put all guidance where people are looking when there is a validation error.
- How do the nudges to create stronger passwords and the problems with users choosing single MFA options combine to create issues in authentication? Are users more likely to run into MFA issues because they have to frequently reset their password?

Finding the “create account” button

5 participants (p5, p10, p11, p12, and p20 initially started typing their email in the sign-in email field. One participant using a screenreader (p10) was significantly held up on the sign-in page. Because they were navigating the sign-in page with the keyboard, they did not find the “create account” button until prompted by the facilitator to try to find it.

Recommendations

- Explore ways to adjust sign-in screen layout so that the 2 options are clearer up front, and in a way that is better suited for a screenreader.

Identity verification issues

Unable to get out of desktop upload page

3 of 21 participants could not figure out how to leave the upload-from-desktop screen when they wanted to. These participants clicked on the upload-from-desktop option but wanted to go back to the previous screen to upload from their phone. The only option they saw on the screen was the “cancel” link, which gave them a warning that they’d need to start the ID verification process over. That warning gave the participants pause. One participant (p13) just proceeded with the desktop upload because they didn’t want to start over.

At this point in the flow, starting over is actually not that big of a deal. That just takes users a few screens back. They have not actually entered any information for the identity verification process. However, after just going through account creation, participants seem to be reasonably concerned that starting over means losing all progress on account creation.

Recommendations

- Give users a clear way to go back to the previous screen (“How would you like to add your state-issued ID?”) or opt to switch over to the phone-handoff flow. There are two improvements that have been considered:
    - Implement a link to switch to the hybrid flow on the desktop “Add your state-issued ID” screen (design complete and low development effort, currently in Team Ada’s icebox): LG-5959
    - Make the browser back button work on the “Add your state-issued ID” step and throughout the IdP. Team Joy has explored the idea[21] that we could:
        - Implement the concept of “milestones” – decide when going back in the flow would be destructive, and at those steps, show a warning screen stopping the user from losing their progress.

[21] Slack update from Team Joy UX and technical findings document on browser back

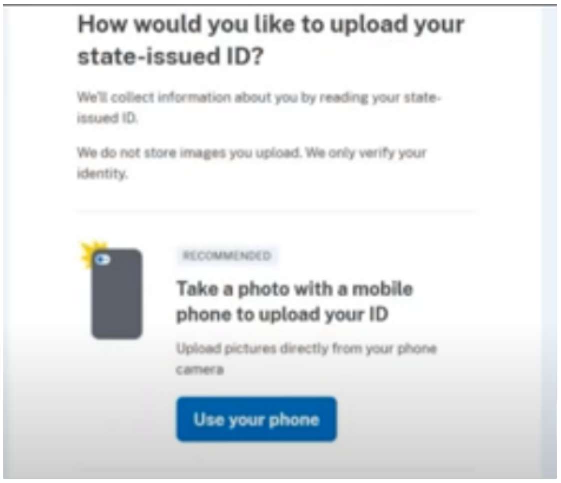
- Currently the system forces the user back to the current step that they are on, so browser back overall does not work. Once we have guardrails in place to prevent users from taking a destructive action unintentionally, we could easily remove this forced redirect functionality for all other steps on the IdP.

Not clear what to expect with the desktop-to-phone handoff

3 participants manually took pictures of their ID before they clicked on the “Use your phone” button on the “How would you like to add your state-issued ID?” screen. The participants were preparing for the next step, not realizing that there was this cool automated experience waiting for them.

Recommendation

- This observation is outdated. Staging seems to be a bit behind the latest UI updates (see right). There is now more text explaining what will happen. Continue to monitor. See LG-5196.



How would you like to upload your state-issued ID?

We'll collect information about you by reading your state-issued ID.

We do not store images you upload. We only verify your identity.

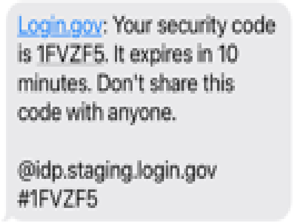
RECOMMENDED

Take a photo with a mobile phone to upload your ID

Upload pictures directly from your phone camera

Confusion on whether to include “#” in SMS code

3 participants were confused about whether they should include the “#” when typing their SMS security code in the appropriate field. At least one participant (p20) included the “#” they saw in the text message. 2 others (p2 and p5) were confused on whether they should but then saw that they couldn’t finish entering the code with the # and took it out. This was not a blocker but created some unnecessary confusion.



Login.gov: Your security code is 1FVZF5. It expires in 10 minutes. Don't share this code with anyone.

@idp.staging.login.gov
#1FVZF5

Personal keys

At least 3 participants (p5, p8, and p11) did not know what a personal key was or why it was important until they found the explainer text. Another participant (p13) knew what a personal key was and did not like having to use them, saying “If I lose it, I feel like I'm going to be.. yah, I get worried about these. If you lose it, you may not be able to unlock your account."[22]

4 participants (p1, p7, p9, and p13) ignored the personal key save options. Instead, they took a picture of the personal key on their phone or with a screenshot on their desktop. 2 of those participants (p7 and p9) said they normally write down with pen and paper things like personal keys, but they did not have a pen nearby. 2 participants (p9 and p13) also mentioned that they would normally store this kind of information in a password manager.

The team also observed that at least 2 participants (p5 and p8) did not save personal keys on their desktop in a way that would make it easy to recall when necessary. This was not a broad pattern, but one participant saved their personal key in a folder called “Savings tips”. Another saved the personal key in a folder called “recipes”. Participants could be doing this because this was just a study with no real-world consequences. If this is actually how these participants would save personal keys, they would likely have issues finding their key when they need it.

Recommendations

- Explore moving links to learn more about personal keys up above the personal key. Very possible this has been considered before.
- Explore ways to encourage better saving locations. Integration with password manager?

[22] Participant 13

Auto-capture took blurry photos

A few participants used auto-capture to upload their photo ID. After properly aligning (supposedly) their photo and getting the auto-capture feature to automatically capture the photo, the participants got an error saying that the image was too blurry.

Recommendations

- Investigate whether the auto-capture tool takes blurriness into account when giving the users the 3-2-1-go and taking the picture. Ideally, blurriness should be a factor in whether the photo is ready to take.
- Investigate if the blurriness threshold can be adjusted without negative consequences to allow more photo through.

Manually uploaded photo ID didn’t meet requirements

5 of 21 participants had an issue manually uploading a photo ID (i.e., not using the auto-capture feature). Participants generally skipped the text explaining how a picture of a photo ID needs to look (e.g., ID is 80% of picture, dark background, etc.). One participant suggested that Login provide visual examples of a good picture of an ID:

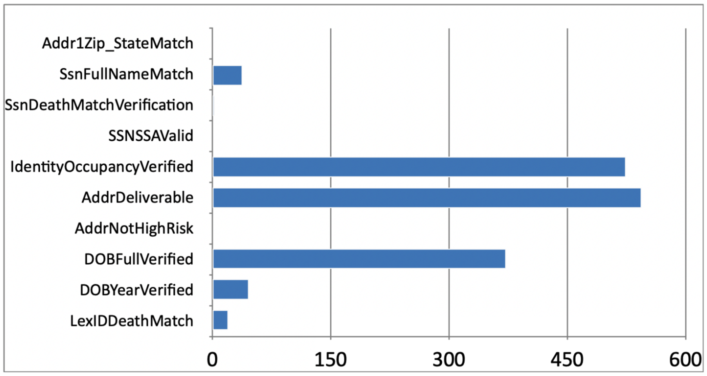
> I think a good tip would be to include an example picture. Here's what we want it to look like. We want it to be large, not so much background. We want it to be very clear with the words. I don't know if you've seen those before, but if I'm here trying to upload it'd be nice to give a sample. Here's John Doe's ID that he uploaded. - p13

Recommendation

- Explore how Login.gov can make ID upload guidance more visual. Can we add an illustration or sample ID photo to help people understand what kind of picture they need to upload?

InstantVerify & Puerto Rico

InstantVerify is terrible with Puerto Rican addresses and dates of birth. The bulk of the errors are IdentityOccupancyVerified, AddrDeliverable, and DOCFUllVerified[23]:



Recommendations

- Report InstantVerify's poor performance to LexisNexis and start a conversation with them about improving the service for PR addresses. Use Identity Transaction Results – Oct 25 - Nov 1, 2022 to support that conversation.
- Investigate whether InstantVerify has a normalized address format for Puerto Rico.
  - If so, how can Login's UI be updated to help users use that format? Or how can the OCR be tweaked to generate that format?
  - If not, what is out there to help validate or normalize PR addresses? Can Login.gov suggest a normalized PR address for submission? Could USPS's Address API help? Are there other options?
- Investigate the date format on PR IDs (is it DD-MM-YYYY or MM-DD-YYYY?) and confirm how InstantVerify reads those dates for DoB. Consider running an experiment with dates from PR IDs, sending the data in DD-MM-YYY and

[23] To grab this data from CloudWatch, run the query in CloudWatch query for Puerto Rico errors in InstantVerify.

MM-DD-YYYY format to LexisNexis Instant Verify and logging the results for both; then, determine if either has a higher success rate.

Other interesting observations

Preference for calling customer support

Participants that sought out customer support information preferred phone over email. This helps validate Login.gov's decision to bring back the customer support phone number.

> "I like to talk to people instead of email, text" - p14

> "I guess I would probably call [customer support] if I was having a real life issue." - p15

Address on ID not actual address

2 participants (p2 and p9) had an address on their photo ID that was not their actual address. Both participants recently moved but did not update their address. In both cases, the participant changed their address to their current address and did not have any issues getting the address verified. Although the participants were a little confused on how to handle the situation, this was not a blocker.

Final thoughts

Through this observational study, the team was able to observe, in real-world, human terms, the impact of some of the issues we've seen in our data, usability testing, and customer support tickets. For some participants, the process was a breeze. For others, there were some bumps, but they made it through.

And yet for too many, they could not use Login.gov because the product was not built with them in mind. They did not have the right ID, their home wasn't in our databases, or they relied on assistive tech we don't fully support (e.g., screenreaders).

For the product issues highlighted in this synthesis, Login.gov has two paths ahead:

1. Get serious about making unsupervised proofing work, or
2. Bring more human judgment into the system.

In the long-term, Login.gov will need to do both to cover everyone.

In the short/medium-term, Login.gov could continue the work needed to improve unsupervised proofing. Different ID upload patterns, a better understanding of users, and more focused procurements could all help Login.gov make the product more usable and accessible. That will improve success rates.

Alternatively, Login.gov could bring humans into the fold through remote identity proofing with supervision and human-in-the-loop. Both options bring greater flexibility to a currently rigid process and would allow Login.gov to expand the types of users it serves.

Either way, Login.gov should work to make the product more flexible and accommodating to users from a variety of backgrounds. By doing so, Login.gov can do what it was always meant to do: get out of the way and help the public connect with their government.

Appendices

Research assets

- The Study Research Plan: Direct Observation Study: Understanding Challenges with Unsupervised ...
- All notes from the sessions (exported from Reframer): Observational Study Notes
- Full list of participants with demographic data and some data analysis used in this report: Participant Tracker + Analysis

Related research

- VPAT Cognitive Disability Testing Report 2022
- VPAT Blind and/or Low-Vision Disability Testing Report 2022