OIX OPEN IDENTITY EXCHANGE

IDENTITY REPAIR IN THE GOV.UK VERIFY FEDERATION

BARCLAYS

experian

GBG

POST OFFICE

Cabinet Office

Department for Work & Pensions

National Cyber Security Centre

DISCOVERY PROJECT REPORT

EDITED BY PENNY NEWTON

MARCH 2017

Contents

Executive summary

Identity theft is estimated to cost the UK over £5.4 billion a year. It occurs when fraudsters access enough information about someone's identity (such as their name, date of birth, current or previous addresses) to be able to impersonate them, or when they steal credentials, such as passwords, and takeover the person's account with a service provider, such as a retailer or bank.

Identity fraud occurs when an individual's stolen identity information or credentials (see identity theft above) are used to obtain goods or services by deception. This can have a direct impact on an individual's credit rating and access to personal finances, as well as having an emotional and psychological effect on them.

Fraudsters generally target 'low hanging fruit' using relatively simple techniques to steal personal data or pass over security details. When a new and stronger security mechanism is deployed, fraud is normally displaced to the next most vulnerable and lucrative target. Organisations typically respond after they have been attacked by raising their customer security protocols. There is some collaboration between organisations to fight the common menace of fraud but the most prevalent response is for each organisation to introduce new and varied methods of security as they are needed. The complexity of navigating these new and differing security protocols is usually born by the user.

GOV.UK Verify was developed to address this spiralling complexity. It allows people to establish a trustworthy digital identity with an Identity Provider and then use it with multiple third party service providers. The Identity Provider must meet high government standards for identity verification at registration of the user and must operate a secure means of authenticating the user's identity in subsequent transactions.

GOV.UK Verify has been built around defined 'levels of assurance' with a set of standards for each of the levels from 0 (no assurance) to 4 (very high). So far it has been deployed at level of assurance 2 (LOA2) which aims to align with legal terminology, identifying a person 'on the balance of probabilities'. Other levels of assurance will be deployed as demand arises and work is being currently undertaken around level of assurance 1 for services which need less proof of identity from users.

Identity systems have the potential for fraud. As adoption of GOV.UK Verify grows, fraudsters can be expected to attempt and possibly succeed at the impersonation of an individual in order to create a digital identity or at 'hijacking' an existing digital

identity account. Identity Providers have in place systems to detect and rectify identity theft should it occur. But when fraud is identified the damage with Relying Parties where the identity has been used fraudulently needs to be repaired.

This report summarises the results of an Open Identity Exchange (OIX) discovery project conducted on the subject of Identity Repair. It explored how users expect an identity repair service to work in a manner that respects their privacy and maintains their confidence in the Verify scheme. The project tested out an online identity repair function, which canvassed users' channel preferences for contact during the interaction- online, telephone or face-to-face, in order to understand which are most appropriate. It also considered how identity repair services should be branded and initiated.

Further work will be conducted following this initial project. When a person suffers identity theft today it is usually their responsibility to detect the scale of the damage and attempt to repair it themselves. In federated identity schemes, such as Verify, once identity fraud has been detected, it can be prohibited from recurring through the compromised digital identity. Development of the concept of identity repair will enable organisations to collaborate to rectify their relationships with users when instances of identity fraud occur.

Introduction and Project Background

Identity theft occurs when fraudsters access enough information about someone's identity (such as their name, date of birth, current or previous addresses) to commit identity fraud. Identity fraud involves the use of an individual's stolen credentials to obtain goods or services by deception. This can have a direct impact on an individual's credit rating and access to personal finances, as well as having an emotional and psychological effect on them.

Identity theft in the UK reached record levels in 2016, with a reported 172,919 cases- the highest number since records began 13 years ago. Identity theft represented 53.3% of all fraud recorded by Cifas (the UK's fraud prevention service) of which 88% occurred online. The age group that experienced the highest increase (+34%) was under-21 year olds. [1] The cost of identity fraud to the UK is estimated to cost over £5.4 billion a year. [2] It takes an individual between 3 and 48 hours of work to try to repair their identities with the worst cases taking over 200 hours.[3]

GOV.UK Verify is working with Relying Parties and Identity Providers to consider how to repair an identity should it be compromised by a fraudster in some way. For example, a user's digital identity account could be compromised, either lost or stolen, or a person's identity details could be used to create a fraudulent account with an Identity Provider. This project aimed to discover if in such instances, a user whose identity has been compromised would be able to 'repair' their digital identity via an online resolution process.
This process would also involve Relying Parties who need the ability to repair the damage caused by these fraudulent transactions within their services, as well as giving the Identity Providers the chance to aid in this process and regain user's trust.

Cases of identity fraud

During the project scoping phase, four scenarios were identified whereby identity fraud could occur:

1. Case of stolen credentials
    - fraudster uses a genuine user's credentials to authenticate themselves to a service, to conduct fraudulent transactions and enable further attacks

[1] http://www.bbc.co.uk/news/uk-39268542

[2]http://www.experian.co.uk/blogs/latest-thinking/fraud-costs-uk-economy-193-billion-year-equating-6000-lost-per-second-every-day/

[3] http://www.aboutidentitytheft.co.uk/identity-theft-facts-figures.html

2. Case of account takeover
    - fraudster takes control of a genuine user's account and replaces their credentials and identity information with fraudulent information, then uses that account to conduct fraudulent transactions and enable further attacks

3. Case of session takeover
    - fraudster takes control of authenticated sessions between a user and a service to enable fraudulent transactions and further attacks without the knowledge of either the genuine user or the service provider

4. An account set up in the name of a genuine person by a 3rd party
    - fraudster uses either genuine or fraudulent identity information to set up an account in the name of a real person and then uses that account to conduct fraudulent transactions and enable further attacks

Rather than test out each of these individual cases with users during the discovery research phase, it was agreed that two high level use cases would be tested in order to gain a deeper understanding of how users felt and reacted to their credentials being compromised.
High level use cases involved two Driver and Vehicle Licensing Agency (DVLA) journeys, one where the user was notified within the system that changes had been made to their driver licence record, and the other, where they received an email from DVLA alerting them to changes they never made.

Methodology

The project focused on the following hypothesis:

'The user will be able to repair his / her digital identity, and transaction history with Relying Parties where it has been used fraudulently by another party.'

A number of objectives were set out to be explored within the project. The project looked to explore the concept of an identity repair centre and also to investigate what a high-level architecture for identity repair could look like. Common terminology and descriptions associated with identity repair needed to be examined. Ultimately, the project needed to test with users, their expectations of what should happen when their digital identity had been compromised.

The project involved a collaboration between the Government Digital Service, NCSC (National Cyber Security Centre, a part of GCHQ), Department for Work and Pensions, GB Group, Experian, Barclays, and Post Office. ID Research conducted the user research and designed the wireframes for testing.

A total of 11 one-to-one usability sessions were run with a selection of users who had either taken place in previous GOV.UK Verify research, or had used GOV.UK Verify live as part of their enrolment in Universal Credit. Given the limited scope of the Universal Credit trial to date (approximately 200k users), and the low recognition of GOV.UK Verify, only two users who could recall using GOV.UK Verify in this context were able to be recruited. The remainder were all users who had used GOV.UK Verify in past research sessions.
The sample was representative in terms of digital literacy and social grade, but was biased in terms of age, with the age range of the group being from 25 to 45 years old.

Research focus

As part of the planning process a number of workshops were run with Identity Providers and Relying Parties to identify and prioritise research questions and hypotheses and define the focus for this research. These fell into two core groups:

Primary research questions

These questions addressed the fundamental issues that needed to be uncovered before the project can move beyond the discovery phase:

1. Can a 'self-serve' digital identity repair service meet functional needs and repair the individual's trust in the federation?
2. Is repair most effective at restoring trust across the federation when taking place with GOV.UK Verify or with an Identity Provider?
3. Can users be guided appropriately into identity repair functions in a purely digital interaction?
4. What channels would be expected for communicating with users during identity repair?
5. What are users' expectations of identity repair?

Secondary research questions

These lower priority questions addressed user issues that were explored within this project:

1. Which elements of digital identity repair build trust?
2. Which elements of digital identity repair damage trust?
3. Whom do users hold accountable for the problems they encounter?
4. What are the drivers of channel preferences during identity repair?
5. Whom does the user want to complete the identity repair?
6. How do users respond to more demanding identity verification in the context of identity repair?

7. Will users be happy to grant access to their data to support identity repair?
8. Given appropriate prompts, will users act to resolve a compromised account?
9. Will users be receptive to learning about preventing identity theft in the context of identity repair?

Research Findings

Findings have been clustered into the following thematic groups and are discussed below: the restoration of trust; where identity repair is effective; expectations & channel preference; users' call to action; and behaviour during identity repair.

The restoration of trust

Can digital identity repair meet users' needs?

Almost all of those users we spoke to felt that their compromised identity had been successfully resolved by the identity repair interaction, and were happy to use GOV.UK Verify to complete further interactions.

One user was not happy to do so, but this objection resulted from discomfort with private sector involvement in government interactions, and was not as a result of concerns around compromised identities or identity repair.

"It would be much easier to use the Verify to apply for a passport. Everything that's happened makes me more confident."

Claire, discussing using GOV.UK Verify after identity repair

Can digital ID repair meet users' emotional needs?

It is less clear whether the digital identity repair interaction could meet all of the users' emotional needs.

Throughout the research, many of the users discussed the need for emotional reassurance, in two main areas:

- Reassurance that their current course of action was the best way to resolve the problem.
- Reassurance that the issue was being appropriately dealt with.

Having been through the identity repair interaction, some felt that they would still want to speak to someone to address these unmet emotional needs.

"Emails are more convenient. Saying that, talking to someone is more reassuring. I'd rather have a phone call if I'm really thinking about it."

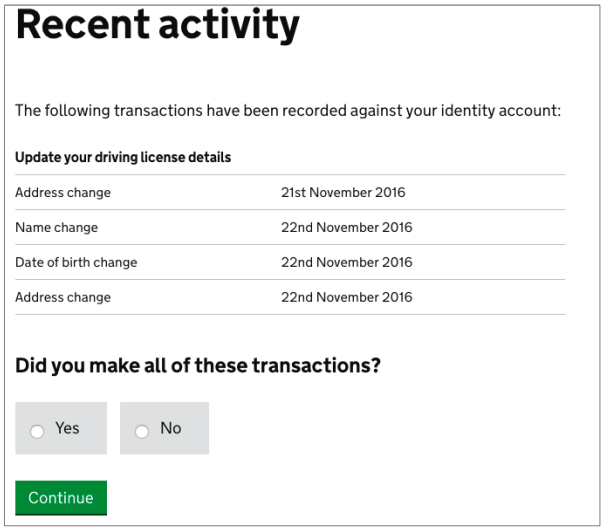
Molly

"It depends on the kind of day I'm having, if I was super shocked, I may not be that relaxed about it [completing identity repair online]. If I spoke to someone and they told me I need to do it online, and it's the quickest way, then I'd just do it."

Davidson

What builds trust?

The most obvious positive impact on trust was encountering the additional identity checks (document and face scanning) to increase the security of an existing account.



Increased visibility and understanding of the status of the issue increased trust.

"Going through it shows me that it's not that simple to get at my information, not without my face."

Claire

Seeing the state of the system and identifying the cause of the problems, also had a positive impact on trust. For example, when users were shown a list of recent transactions recorded against their identity account.

Users also reported increased feelings of trust and security when they felt a sense of control over the interaction, such as being offered the ability to report problems online or by phone, or being able to select preferred contact channels.

What damages trust?

The most significant negative impact on trust was when users were asked to create a new identity account. Although it had been stated that this account would provide a higher level of security, users felt it would in fact expose them to more risk.

"This is going nowhere. This is a mess. It would be better to call them. You've already gone through this, and it's obviously generated some kind of fraud, and it didn't work in the first place. I'm being asked to create multiple verification accounts with different companies, I thought it would take five minutes and it's going to take much longer. This is what makes me reluctant to use the whole online thing."

Jacob

It was also clear at this point that users were confused and had lost much of the positive sense of understanding and control provided earlier. This led them to consider the process more carefully and to focus on negative perceptions.

This effect has been observed in previous research. Those users who progress without experiencing usability or comprehension issues were more likely to maintain a sense of flow – being fully immersed and involved in their task - and less likely to question aspects of the process that were more challenging for others.

"Oh for God's sake…I'm tired…I'm bored now…I'd come back to this another day…Oh my word…This wouldn't have happened if I hadn't done it in the first place, is it worth me creating an account and opening myself to these possibilities?
Is it really worth it?
It's great when it works, but when it goes wrong…"

Molly

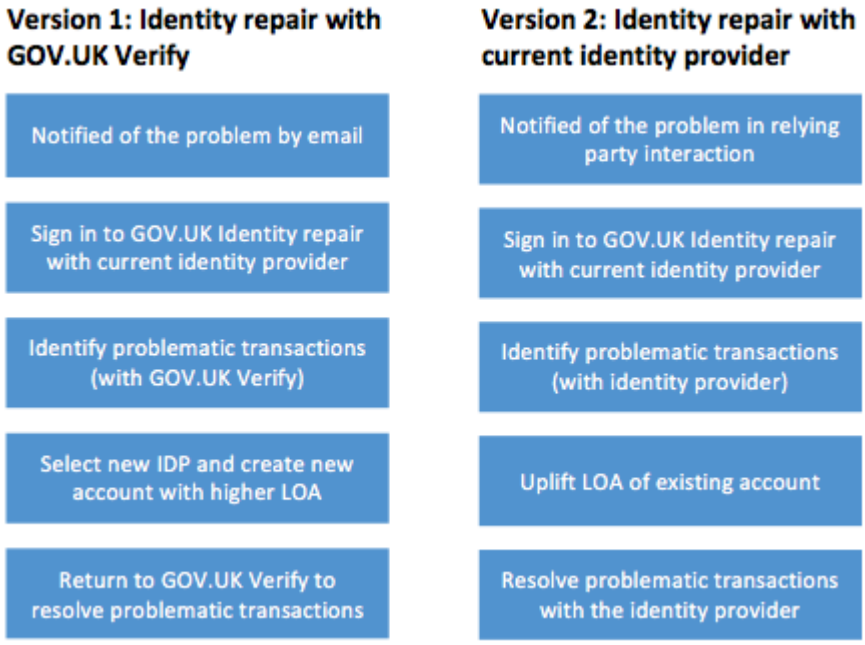
Familiarity, convenience and trust

When considering reuse of a GOV.UK Verify credential after the identity repair interaction, most discussed familiarity and convenience as the drivers of their choice. Users were both more familiar and more trusting of GOV.UK Verify after identity repair, but it was familiarity that proved to have the greatest impact on willingness to reuse their identity account.

Where is identity repair most effective?

Identity repair with GOV.UK Verify vs. identity repair with Identity Providers

During research two different user journeys were tested. These journeys differed in terms of where the identity repair took place and whether the user had to create a new identity account with a higher level of assurance (LOA) or increase the LOA of their existing account.



It was clear from the findings that version 2 presented fewer challenges and led to better outcomes. In the most part, this was due to confusion over why users were being asked to create new identity accounts in version 1.

Most users attributed blame for unauthorised transactions to the Relying Party, not to GOV.UK Verify, and therefore did not understand the need to create a new identity account. As a result, most simply chose the same Identity Provider as before, often citing the same reasons as for their original choice.

> ***"I thought I had an account already, didn't I say I had one? So I'm creating an account with Barclays. I thought I was just checking my details, not actually creating a new account. I would just continue with the same company."***
>
> Lee

These differences in perceptions and outcomes can be summarised as follows:

- **Version 1**: Users felt they were creating another, similarly vulnerable identity account and did not understand why.

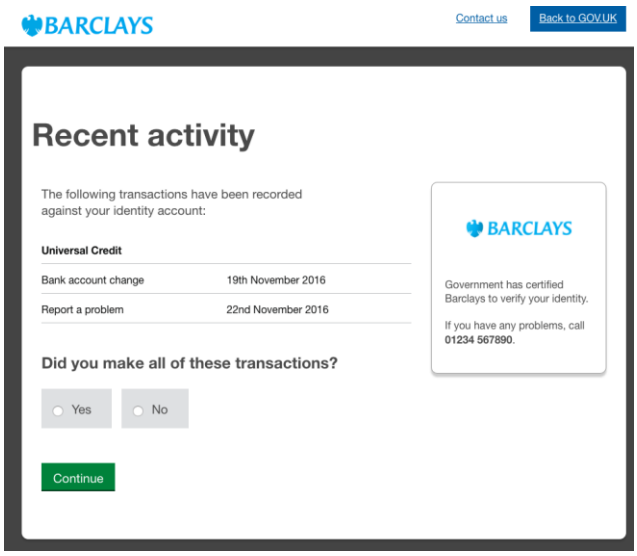
- **Version 2**: Users understood that they were increasing the security of their existing account in response to the problems encountered.

The challenges of repairing a compromised account

Although version 2 presented fewer issues for users and generally led to better outcomes, some users raised concerns about how a potentially compromised account could be secured. The prototype did not fully address the issue of creating new access credentials (username, password and 2nd factor authentication).

This part of the interaction has the potential to add significant complexity and confusion and should be explored as a priority in future iterations.

Branding and responsibility for repair



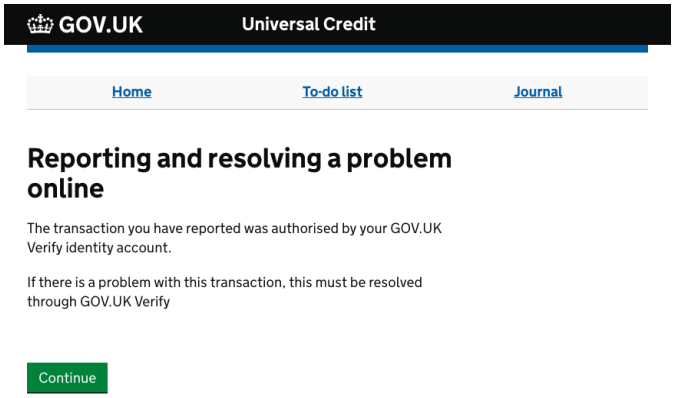
Branding elements used for identity provider prototypes did not always lead users to understand where they were.

Though it was clear that users experienced better outcomes with version 2, many still believed that GOV.UK Verify had carried out the identity repair.

Prototypes of identity provider interactions used minimal branding and shared common form elements with GOV.UK, which may have added to this perception.

This also suggests that users expected this part of the interaction to be managed by GOV.UK and that the minimal branding was not sufficient to overturn that expectation. If that is the case, then later iterations should feature clearer identity provider branding and subsequent research should pay attention to the potential for issues arising from this.

Responsibility for account compromise



Prototypes attributed the cause of problems to GOV.UK Verify, however most users did not see it that way.

Although the prototype attributed the cause of the problematic transactions to GOV.UK Verify, by the end of the transaction most users did not.

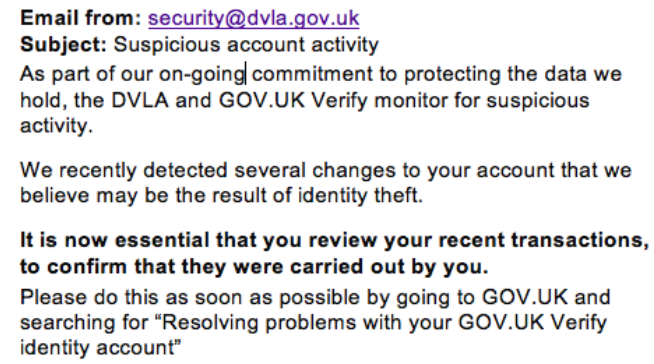
During the earlier stages of the interaction many users were hopeful that the issues identified with their account resulted from an innocent error and appeared unwilling to assume that this was the result of malicious action.

When pushed to attribute responsibility for the initial problem and for its resolution, most felt that the problem had been caused by the Relying Party and fixed by GOV.UK Verify. Most also thought the Identity Provider was only responsible for verifying their identity, and did not see their involvement in authorising these problematic transactions.

A common factor for all of the prototypes was that after initially identifying a problem users are taken away from the Relying Party to repair the identity with either GOV.UK Verify or with the Identity Provider. This prevented any opportunity for re-establishing users' trust in the Relying Party and suggests that the Relying Party should have a greater presence in the repair process if this relationship is to be repaired.

Expectations & channel preference

What do users expect to happen?



Email from: security@dvla.gov.uk
Subject: Suspicious account activity
As part of our on-going commitment to protecting the data we hold, the DVLA and GOV.UK Verify monitor for suspicious activity.

We recently detected several changes to your account that we believe may be the result of identity theft.

It is now essential that you review your recent transactions, to confirm that they were carried out by you.
Please do this as soon as possible by going to GOV.UK and searching for "Resolving problems with your GOV.UK Verify identity account"

Email notification of suspicious account activity was effective at alerting users to the issue.

Regardless of how users were notified of a problematic transaction, most seemed reluctant to jump to the conclusion that this was the result of malicious action. Rather users preferred less threatening explanations such as a mistake during data entry.

Having been alerted to a problem everyone expected it to be resolved by the Relying Party where they had initially experienced it. Although all users had previous experience of GOV.UK Verify, none had sufficiently refined understanding of how GOV.UK Verify worked to even consider that other parts of the GOV.UK Verify federation might be able to respond to the problem.

Initial channel preferences

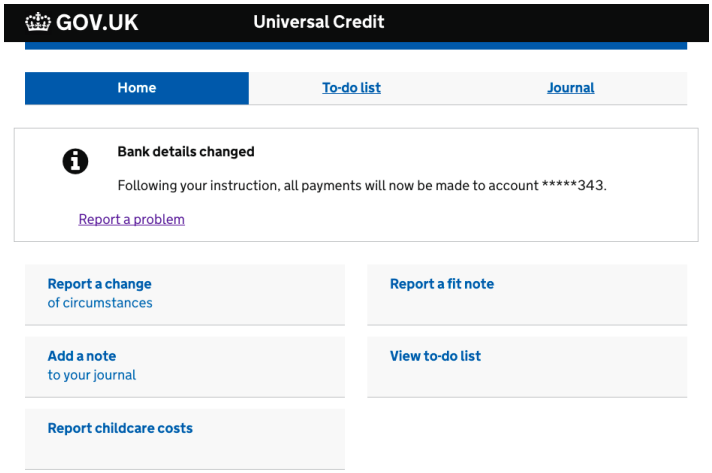
Those alerted to the problem by email were more likely to report they would contact the Relying Party by telephone.

> ***"I wouldn't go online, as it's not secure. I'd call them, as I'd want to speak to a human being. There should be a contact number on the DVLA website, so I could tell them about the email and tell them that I was uncomfortable doing that online."***
>
> Molly

Although those reading the email were clearer about what had happened, they were less likely to follow instructions given.

It was clear that the instructions in the email were not guiding people to the right place. For example, when asked how they would respond to this problem online users suggested a wide variety of approaches and only a few reported they would

actually follow the instructions in the email.



Users were notified in the interface that an unauthorised change had been made. This was missed by some, but more effective at routing those who did see it to the right place.

Those users alerted as part of the interaction were more likely to follow the link provided, taking them to the right place to resolve the problem online. However, these users were less likely to understand the severity of the issue.

Some had to be prompted to read the notification shown in the interface and a few felt that the link *'Report a problem'* sounded like it was for reporting problems with the website and was not for problems of this severity.

Expected response time drives channel choice

The current Universal Credit claimants spoken to were wary of reporting the problem online. These users felt that the response times they usually experienced through the Universal Credit interface were too slow for such an important issue. When presented with an option to resolve the issue by phone or online, these users chose the phone for this reason.

Emotional drivers of channel preference

Most users reported they would rather report and resolve this issue by phone. The most common reason for this was to seek reassurance that:

a. they were dealing with the problem in the most effective way;
b. the problem was being dealt with effectively.

These concerns should be addressed more effectively early on if this preference is to be altered and users are encouraged to complete this interaction online.

Calling users to action

Usability of email notifications

The findings of this research demonstrate significant issues with email notifications. Users who saw the notification were unlikely to follow the instructions in the email, with many reporting they would phone the Relying Party. Some also said that they would expect the email to contain a link.

This suggests that email notifications have limited effectiveness, whilst also presenting a significant opportunity for phishing.

Challenges of in-page notifications

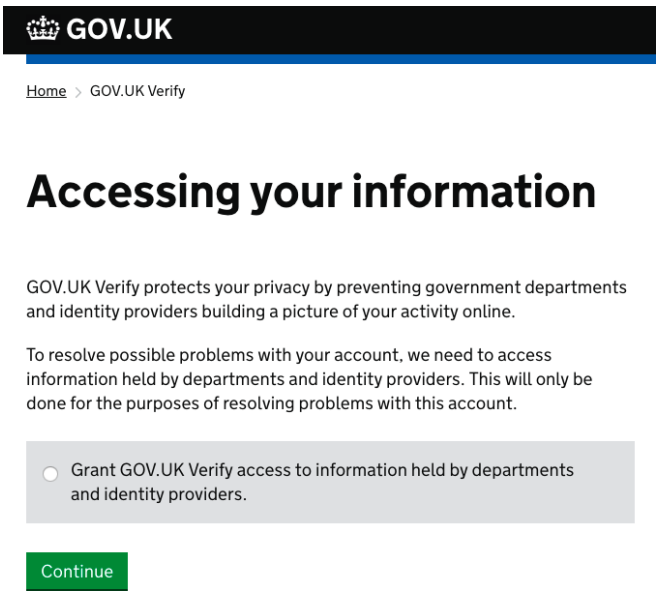
It was clear that the in-page notification used in the prototype (shown above) was not up to the task.

Some users spent a considerable amount of time exploring the page without noticing it and some did not see it at all until prompted. It is clear that such an important message must command more attention.

Some users were concerned as they felt that they had only noticed the issue by chance and that if they had not visited the website the problem would have gone unreported, suggesting users see the Relying Party as being responsible for monitoring the account and notification of changes.

Behaviour during identity repair

Granting access to data to support identity repair



Though willing to grant permission for data sharing, the

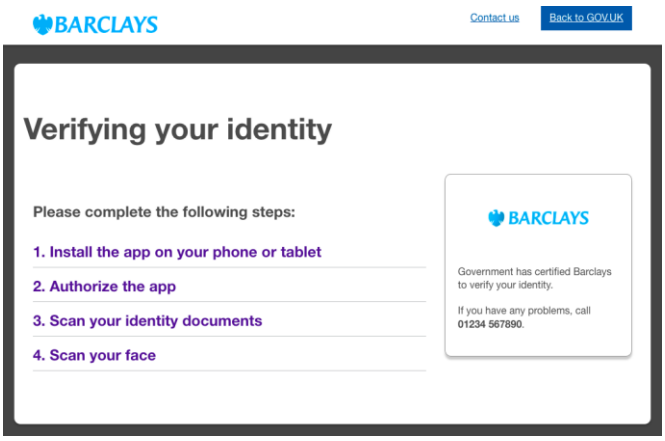
supporting copy confused some users.

Few users had any objection to granting permissions to extend data sharing to facilitate the identity repair. There was no discernible difference in willingness between granting permission to GOV.UK Verify and granting permission to an Identity Provider.

Although happy to grant permission, some struggled to understand the why this information wasn't already accessible. Some users interpreted the first paragraph of this page (shown above) as meaning that government departments and Identity Providers could not be trusted with personal information and therefore might be responsible for the problems experienced.

"Protect your privacy by preventing Government departments and identity providers? That's a bit contradictive. Why's it protecting that? ... Maybe it's* [my account has been compromised by] *someone in Government or an identity provider, or an Internet scammer. I imagine it's someone who has certain levels of access."

Lee



Most users understood the need for higher levels of verification.

Higher levels of verification during identity repair

As part of the identity repair interaction users were told they would need to verify their identity to a higher level than before. This interaction was simulated with a simplified process to install an app, scan an identity document and then scan their face.

Those users doing this to increase the security of their existing account generally had fewer issues with the process.

"The situation warrants the invasiveness"

Kat

Those users doing this as part of creating a new identity account tended to have more objections. These highlighted issues are often heard with app-based document scanning, for example:

- Users were unwilling to install the app.
- Users were unwilling to keep infrequently-used apps on their phone and were concerned what impact this may have on their identity account.
- Users raised privacy concerns about uploading images of their identity documents and their face.

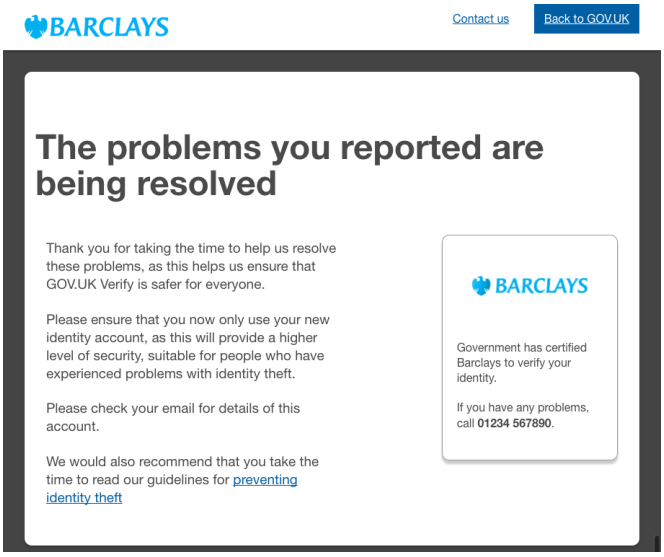
"The face scanning, I'd like to delete that. The whole app. I wouldn't want it on my phone once I'd sorted that issue."

Paris

"I'd stop here and call. Driving license? No! Passport as well? No way! That's putting all your eggs in one basket. No way. The reason I'm here is that someone's hacked my account. It's not going to happen. What about people like me that change hair and glasses all the time? Would it say that it's not me? What happens then?"

Molly

Response to prevention content



Most users wanted to know more about preventing identity

At the end of the identity repair interaction users were shown a page summarising the outcome of the interaction. At the bottom of this page there was a link to *'preventing identity theft'*.

Almost all users who reached this page tried to click on this link to learn more.

Though there is no indication that such content would be effective at changing behaviour, this at least shows that users are willing to learn more, and do not object to the idea that they might take responsibility for reducing identity theft.

Content for this topic should be included and refined in further iteration.

Conclusions

The project set out to discover if a user would be able to repair their digital identity and transaction history with Relying Parties, where it had been used fraudulently by another party.

The conclusion reached is that most users felt that their compromised identity had been successfully resolved by the designed identity repair interaction, and were happy to use GOV.UK Verify to complete further interactions.

Most users initially reported they would prefer to complete this process over the phone. However, having been through the online process most were still confident in using their identity accounts with GOV.UK Verify.

One key factor influencing outcomes was whether users repaired a compromised identity account or created a new one. Those who created new accounts often felt this put them at more risk, and these users tended to have more negative outcomes and less trust within the process. Those that repaired compromised accounts felt they were better protected.

The most obvious positive impact on trust within the identity repair function was encountering additional identity checks (document and face scanning) to increase the security of an existing account.

Most users attributed blame for unauthorised transactions to the Relying Party, not to GOV.UK Verify, and therefore did not understand the need to create a new identity account- rather they chose the same identity provider as before.

Recommendations

There were a number of points that arose during the user testing which should be addressed in any future work on this topic, and are listed below:

- Users needed better reassurance at the beginning of the identity repair journey - that the repair function was dealing with the problem in the most effective way and being dealt with efficiently. This could also alleviate most users needing to call someone at a point in the journey.

- During the user testing, the issue of creating new access credentials (username, password and 2nd factor authentication) when users were asked

to create a new identity provider account was not fully addressed. This part of the interaction has the potential to add significant complexity and confusion. However, the factor that damaged trust in the identity repair process occurred when users were asked to create a new identity account. Repairing a current identity account resulted in better outcomes for users and so any further development in a prototype service should focus on this journey.

- It was clear that the instructions in the email alerting users to an identity breach were not guiding users to the right place. These either need to be made clearer or an alternative way to alert users needs to be investigated.

- As the blame for the fraudulent activity was attributed to the Relying Parties and not GOV.UK Verify or the Identity Provider, further investigation is needed on how this blame should be resolved. Opportunities for Relying Parties should be presented along the identity repair journey to enable them to re-establish this trust with users.

- At the end of the identity repair journey, most users clicked on a link that encouraged them to learn more on how to protect their identities. This willingness to learn more is indicative that users might take responsibility for reducing identity theft and therefore content for this topic should be included and refined in further prototype iterations.

- It is anticipated that this collaborative project will lead onto an alpha project that will design and refine the identity repair function.

Appendix A

Glossary

GOV.UK Verify: GOV.UK Verify is the way to prove who you are online. It gives safer, simpler and faster access to government services like filing a tax return or checking the information on a driving licence.

Identity Provider: This is a certified company that that has met government and industry standards to provide identity assurance services as part of GOV.UK Verify. There are currently seven Identity Providers who can prove users' identities. Also referred to as certified companies.

Relying parties: These are government services in which users can access online with their digital identity, using GOV.UK Verify. For example, these can include checking your state pension or viewing your driver's licence information. Currently there are 12 services available, with more to be added in the future.

GOV.UK Verify federation: This encompasses all parties involved in the creation of a UK digital identity- the Relying Parties, the GOV.UK Verify journey and the Identity Providers.

Level of Assurance (LOA): There are four levels of identity proofing, each of which provide an increasing level of confidence that the applicant's claimed identity is their real identity. Level of Assurance 2 is used in GOV.UK Verify. This is a claimed Identity with evidence that supports the real-world existence and activity of that identity.

Discovery project: These projects are conducted to find out user needs, what to measure and what the constraints are. The project is used to find out how to develop a new service if there is a user need for it.

Alpha project: Alpha projects build on discovery projects and generally involve building a prototype, testing it out with users, demonstrating technical viability and learning from this. Iterations from these findings are then used to design and launch a beta phase.

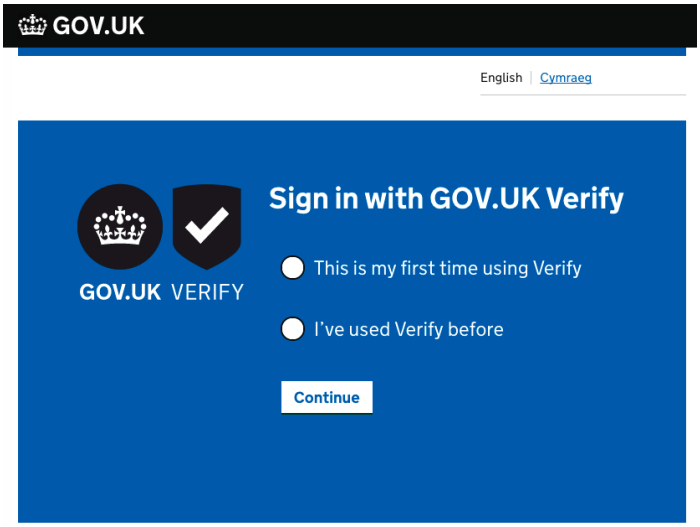
Appendix B

User research findings outside of the original project scope

Recognising GOV.UK Verify and re-using identity accounts

Although not part of the original focus for this research, significant findings emerged relating to how past users of GOV.UK Verify behave when using the service for a second time.

These behaviours varied significantly between those who had used GOV.UK Verify in the real world and those who had used it under lab conditions. However, this difference is most probably the result of bias introduced during recruitment.



The first page of the hub asks users if they have used Verify before.

Recruitment bias

Two groups were recruited to take part in this research:

- Those who had used the live GOV.UK Verify service as part of their interaction with Universal Credit.
- Those who had used a GOV.UK Verify prototype in past user research sessions.

As not all Universal Credit users have used GOV.UK Verify, one of the screening questions used during recruitment of the first group asked if they had used GOV.UK Verify. As a result, a biased sample of users were recruited who remembered using

GOV.UK Verify.

The second group was recruited from lists of past research attendees. Though this group had used a prototype in research, rather than the live service, the bias of the first group was able to be avoided.

Recognising GOV.UK Verify

Several users from the second group above failed to recognise GOV.UK Verify at the first page of the hub, raising significant concerns about the effectiveness of this page.

> ***"I'd go to 'first time'. This isn't the same as before. You could use Barclays, Post office, Experian and those things."***
> Molly

Users who progressed down the 'first time' path recognised GOV.UK Verify at the point where they saw the logos of the Identity Providers. However, as this occurred some pages after the initial question, none went back and changed their initial choice.

Understanding GOV.UK Verify concepts

In addition to these problems with recognition, it was also clear that users returning to GOV.UK Verify did not always remember how it worked, and had little recollection of concepts such as 'certified company' and 'identity provider'.

It appears that it is not enough to simply assume that those who have used GOV.UK Verify before will understand it, and this hypothesis may lead to alternate design solutions for re-use of GOV.UK Verify credentials.