F1457 A1 Equality Impact Assessment (EqIA) form

N.B: the completed form should be emailed to the Diversity and Inclusion team

Project * Programme Strategy Policy*	Single Sign On (SSO) Security

Accountable	Job Title*	Name
	Head of Payments Products Transformation	Andrew Anderson Date 30/09/2020

Produced By	Job Title	Name
	Product Managers Signature	Isabel Hodgson Zivana Lima Date 24/09/2020.

Reviewed By	Job Title	Name
	Head of Payments Products Transformation Signature	Andrew Anderson
	Job Title	Name
	Signature	Date

Document History	Version	Date	Summary of changes
	0.1	24/09/2020	First draft
	0.2	30/09/2020	Final copy

* Delete as appropriate (the Accountable person should always be at least one management level higher than the Responsible person).

Project Related Documents	Doc No.	Document title	Relevant Section(s) of this Document

Step 1: Clarifying Aims

Q1. Outline the aims/objectives/scope of this piece of work

Oyster and Contactless web and mobile applications, as well as the Travel Alerts are authenticated by Single Sign On (SSO) to give customer secure access to their account and protect personal data. The existing framework was developed in house and, following an incident in August 2019 where we noticed fraudulent activity in a number of customer accounts, we are required to update the SSO with a more robust long-term solution to secure the system from unwanted access.

This project will integrate TfL's in-house SSO platform with an off-the-shelf SaaS solution (Microsoft's B2C product). B2C will replace the existing bespoke SSO authentication layer and implement industry standard authorisation protocols (Open ID Connect).
This work will allow TFL to benefit from the robust security features offered by B2C (progressive authentication, Multi Factor Authentication and risk based conditional access) and a best in class approach to identity management.

The work will enable added security features to refunds, that was specifically targeted during the incident in August 2019 when a number of customer accounts were targeted through 'credential stuffing'. As refunds are part of the legacy Oyster Online website a further stream of work will create a new, modernised Oyster refund microservice. This will then be integrated with B2C and allow us to make use of the MFA (Multi Factor Authentication) feature within B2C. Meaning an MFA challenge is presented to customers ahead of any refund request.

By making these changes, we will also be able to restore the online refund self-service functionality, which was turned off because of the security incident last year. This will reduce the number of customers contacting CCO. Based on June's data, this was around 200 contacts per day relating to product refunds.

The addition of a MFA challenge to refund requests was mandated by the National Cyber Security Centre (NCSC) and TfL have committed to the Information Commissioner's Office (ICO) to complete that work as a direct action in response to the security incident.

Q2. Does this work impact on staff or customers? Please provide details of how.

Both Customer Contact Operations (CCO) staff and TfL customers currently use SSO to log into a customer record (either directly or, in the case of staff, on behalf of a customer). The integration of SSO with B2C will not significantly change the way that staff or customers access their accounts, however the MFA related processes will impact users.

An email and password combination will be required for basic access to an account through which they can access all current functionality, apart from personal or financial data (ie profile or Oyster refund). Completing these actions will now require a customer to set up and complete an MFA challenge.

In order to set up MFA, customers will need to provide us with their mobile phone number. When setting up the SMS based MFA touchpoint, the user will need to have access to a mobile phone. They will also require access to that same device when viewing/updating profile information or requesting a refund of a season ticket or PAYG balance.

CCO staff will follow a different identity and verification process (eg asking specific questions to the caller) to access the personal information or request a refund on behalf of a customer. So, the impact on CCO is minimal.

Step 2: The Evidence Base

Q3. Record here the data you have gathered about the diversity of the people potentially impacted by this work. You should also include any research on the issues affecting inclusion in relation to your work

Consider evidence in relation to all relevant protected characteristics;

- Age
- Disability including carers[1]
- Gender
- Gender reassignment
- Marriage/civil partnership
- Other – refugees, low income, homeless people
- Pregnancy/maternity
- Race
- Religion or belief
- Sexual orientation

An important consideration is access to online digital services overall. Recent research shows across the UK online penetration remains at almost 51m users (April 2020), which is over 95% of the adult population. The use of digital services is also increasing, the UK population spent an additional 54bn minutes online in April than they did in February. This is an encouraging trend and allowing TfL customer to manage their travel, payment and ticketing service online may well improve the overall access to travel.

More specifically, the "Travel in London: Understanding our Diverse Communities Report 2019" reports access to online services and smart phone devices based on race, gender, sexual orientation, age and lower income (see 'Access to information' sub section for each headline group). The statistics for all groups showed very high access to the internet at home (99-100% for

[1] Including those with physical, mental and hidden impairments as well as **carers** who provide unpaid care for a friend or family member who due to illness, disability, or a mental health issue cannot cope without their support

all). However, there is some variation when it comes to access to a smartphone and/or the TfL website on a mobile device for disabled customers or those on lower incomes:

1. Lower income access:

Proportion of Londoners who use a smartphone (iPhone, Android, BlackBerry, other) (autumn 2017/spring 2018) [14]

%	All online Londoners	DE online Londoners
Base	(2,062)	(351)
Uses a smartphone	84	76

2. Disabled customer access:

Proportion of online Londoners who use a smartphone (iPhone, BlackBerry, other) (autumn 2017/spring 2018) [14]

%	All	Disabled	Non-disabled
Base	(2,001)	(268)	(1,688)
Uses a smartphone	84	73	87

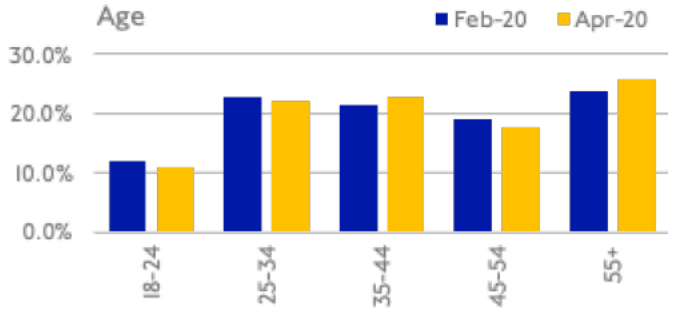
Proportion of mobile phone owners who have ever accessed the internet on their mobile device among online Londoners (autumn 2017/spring 2018) [14]

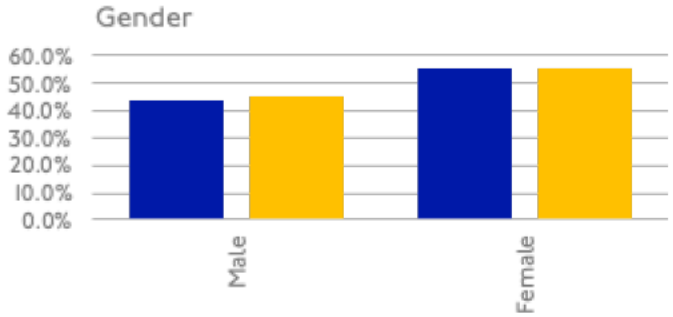
%	All	Disabled	Non-disabled
Base	(1,802)	(225)	(1,539)
Ever accessed the internet on a mobile device	91	86	93

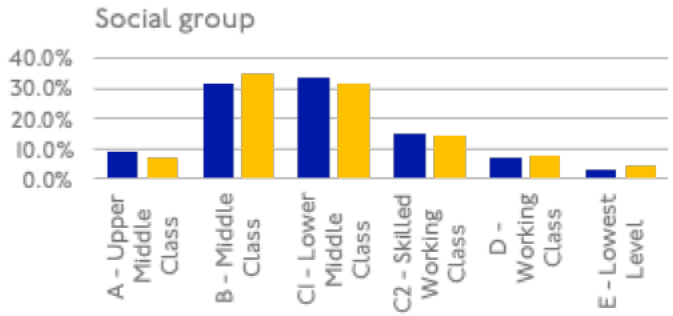
In the context of the SSO Security project, this suggests there may be more barriers for disabled individuals or those on lower incomes to complete an SMS MFA challenge, compared to the general population. Although it is worth noting that any mobile phone can receive an SMS, so when including these devices (alongside Smartphones) we would expect numbers with access to increase. If, however, customers do not own a mobile phone at all, they can call Customer Services to access information in their accounts. In addition, disabled persons are eligible for a Borough issued Freedom Pass, which gives them free travel at all times and also does not require them to have an online account.

TfL take accessibility of all digital services very seriously and are required by law to uphold Accessibility Standards (WCAG 2.1 AA). By adhering to these regulations, we ensure our services do not discriminate and a broad range of customer accessibility needs are met (see presentation in appendix). The project requirements specify adherence with WCAG 2.1 AA and the services will be tested prior to go live to ensure Web Accessibility.

The online account is used by 600,000 customers per month. We cannot identity from website analytics the breakdown of user characteristics however supporting regular 'tracker' research for the digital travel information sector as a whole, we can see total users breakdown in the following ways:







Overall the evidence suggests good access to digital, internet enabled devices and therefore the TfL website. TfL is constantly seeking to remove inequalities and enable accessibility – and so remove barriers to access. The online customer account doesn't present specific issues based on protected characteristics, but the addition of an MFA SMS based challenge may impact some users.

Step 3: Impact

Q4. Given the evidence listed in step 2, consider and describe what potential short, medium and longer term negative impacts this work could have on people related to their protected characteristics?

Protected Characteristic		Explain the potential negative impact
Age	**N**	No anticipated specific impact on this group. Research suggests that both older and younger customer have access to the internet and smart phones.
Disability including carers	**Y**	Research suggests there could be reduced access to a device that would enable a disabled person to receive and respond to an MFA challenge sent via SMS. Therefore, requiring a disabled customer to contact Customer Services in order to access and update profile information or request an Oyster refund. In addition, disabled persons are eligible for a Borough issued Freedom Pass, which gives free travel at all times. Eligible non-Londoners can get an ENCTS pass, which gives free bus travel in London (limiting the need to use Oyster card and therefore reducing the need to sign up for an online account).
Gender	**N**	No anticipated specific impact on this group.
Gender reassignment	**N**	No anticipated specific impact on this group.

Marriage/civil partnership	**N**	No anticipated specific impact on this group.
Other – e.g. refugees, low income, homeless people	**Y**	Low income - Research suggests there could be reduced access to a device that would enable those on low incomes to receive and respond to an MFA challenge sent via SMS. Therefore, requiring a low-income customer to contact Customer Services in order to access and update profile information or request an Oyster refund.
Pregnancy/maternity	**N**	No anticipated specific impact on this group.
Race	**N**	No anticipated specific impact on this group.
Religion or belief	**N**	No anticipated specific impact on this group.

Sexual orientation	**N**	No anticipated specific impact on this group.

Q5. Given the evidence listed in step 2, consider and describe what potential positive impacts this work could have on people related to their protected characteristics?

Protected Characteristic		Explain the potential positive impact
Age	**N**	No anticipated specific positive impact on this group. The main positive impact is improved account security for all our customers.
Disability including carers	**Y**	The project will deliver improved web accessibility of some features in the account area (sign up, sign in, profile and refunds) Although, the main positive impact is improved account security for all our customers.
Gender	**N**	No anticipated specific positive impact on this group. The main positive impact is improved account security for all our customers.

Gender reassignment	**N**	No anticipated specific positive impact on this group. The main positive impact is improved account security for all our customers.
Marriage/civil partnership	**N**	No anticipated specific positive impact on this group. The main positive impact is improved account security for all our customers.
Other – e.g. refugees, low income, homeless people	**N**	No anticipated specific positive impact on this group. The main positive impact is improved account security for all our customers.
Pregnancy/maternity	**N**	No anticipated specific positive impact on this group. The main positive impact is improved account security for all our customers.
Race	**N**	No anticipated specific positive impact on this group. The main positive impact is improved account security for all our customers.

Religion or belief	**N**	No anticipated specific positive impact on this group. The main positive impact is improved account security for all our customers.
Sexual orientation	**N**	No anticipated specific positive impact on this group. The main positive impact is improved account security for all our customers.

Step 4: Consultation

Q6. How has consultation with those who share a protected characteristic informed your work?

List the groups you intend to consult with or have consulted and reference any previous relevant consultation?[2]	If consultation has taken place what issues were raised in relation to one or more of the protected characteristics?
IDAG	• For older people: figures for using internet data questionable. More in-depth research needed. • Investigate to go above and beyond WCAG (not just do minimum), particularly for visually impaired. • User testing for visually impaired and for some physical disability (ie. Disabled persons who cannot use mobile device/computer screen) • Investigate additional alternative methods of contact – email, web chat etc.

[2] This could include our staff networks, the Independent Disability Advisory Group, the Valuing People Group, local minority groups etc.

Q7. Where relevant, record any consultation you have had with other projects / teams who you are working with to deliver this piece of work. This is really important where the mitigations for any potential negative impacts rely on the delivery of work by other teams.

N/A

Step 5: Informed Decision-Making

Q8. In light of the assessment now made, what do you propose to do next?

Please select one of the options below and provide a rationale (for most EqIAs this will be box 1). Please remember to review this as and when the piece of work changes

1. Change the work to mitigate against potential negative impacts found	
2. Continue the work as is because no potential negative impacts found	
3. Justify and continue the work despite negative impacts (please provide justification)	Account use by disabled customers is lower due to the Freedom Pass and the free travel it provides. This means the users do not need to use the online services and payments etc in the same way as those customers who pay for travel. We also know from Dial-a-ride user research it is usually carers or family members accessing online services on the behalf of the disabled customer – a behaviour trend that will further mitigate the issues a SMS based MFA challenge may present. In addition, we will investigate the option to set up an email-based MFA touchpoint in the future. However, the conclusion is that the broader impact of taking steps to protect all customers' data outweighs any potential negative impact on this group
4. Stop the work because discrimination is unjustifiable and no obvious ways to mitigate	

Step 6: Action Planning

Q9. You must address any negative impacts identified in step 3 and 4. Please demonstrate how you will do this or record any actions already taken to do this. Please remember to add any positive actions you can take that further any positive impacts identified in step 3 and 4.

Action	Due	Owner
Accessibility Testing of the new features	March 2021	Isabel Hodgson

Step 7: Sign off

Signed Off By	**EQIA Author**	Name Job Title
	Signature	Date
	EQIA Superuser	Name Job Title
	Signature	Date
	Senior accountable person	Name Job Title
	Signature	Date
	Diversity & Inclusion Team Representative	Name Job Title
	Signature	Date

8. Appendix

Digital Accessibility.pdf