Business Rules & Logic for Lockouts

ℹ There are 4 key scenarios that are off high priority and are treated as an MVP for what GOV.UK One Login’s business rules should be, that are also being driven by a HMRC requirement

Specifically HMRC have a requirement whereby they would like to increase the lock out period from 15 minutes to 2 hours.

The 4 key scenarios are:

1. Create account
2. Sign in
3. Password reset
4. 2FA Account recovery

ℹ Additional info : when we talk about 'lockouts' this does not mean the GOV.UK One Login as a whole is locked. It means the user is locked out from doing the step they were on when they triggered the lockout.
So if a user is signing in, and enters the wrong password 6 times, they won't be able to enter their password for 2 hours.
But if a user has gone down the password reset journey, and enters the wrong email code 6 times, they won't be locked out from entering a password should they suddenly remember it, they will just be locked out from being able to request another email code on the pw reset journey.

What is Time To Live (TTL)?

In addition to the lockout rules, there's a Time To Live (TTL) feature that governs the duration during which a user's sign-in attempts remain valid before triggering a lockout. Currently, the TTL is set to 15 minutes, apart from the sign in journey password entry journey, which is at 2 hours. With the current TTL of 15 minutes, a user has that time window to attempt signing in, with a maximum of 6 password attempts. If they make 5 incorrect attempts within this 15-minute TTL period, they can simply wait until the time elapses. Once the TTL expires, they regain the ability to attempt signing in with another 6 attempts. However, this setup presents a vulnerability, as users can exploit the timer reset to evade the lockout consequences. It is also worth noting that this feature is not public knowledge and so a user would not know that there is a timer that restarts. See TTL rules for a insight into the rules and explanation.

Count TTL vs OTP TTL

OTP TTL:
Time to live for the OTP code, indicating how long the code is available to the user until it expires.

Count TTL:
Time to live for the number of unsuccessful attempts a user has to enter the OTP. If the count expires, the user gets another round of attempts to enter the OTP again.

Importance of Alignment

The goal is to ensure that the Count TTL and OTP TTL are aligned. This alignment ensures that both the OTP validity period and the number of attempts reset at the same time, preventing exploitation.

Example Scenario

Misaligned TTLs

- **OTP TTL**: 1 hour
- **Count TTL**: 15 minutes
- 6 attempts before lockout

In this scenario, the code is valid for 1 hour, and the user has up to 5 attempts to enter the OTP within each 15-minute window. After 15 minutes, the count resets, giving the user another 5 attempts.

Exploitation of Misalignment

A savvy user could exploit this misalignment by:

1. Entering 5 incorrect OTP attempts within the first 15 minutes.
2. Waiting for the count to reset after 15 minutes.
3. Repeating this process every 15 minutes for as long as the OTP code is valid. In this instance 1 hour.

By doing this, the user could effectively gain up to 20 attempts within the 1-hour validity period of the OTP, significantly increasing the chances of brute-forcing the correct OTP.

Solution: Aligned TTLs

By aligning the Count TTL with the OTP TTL, both the OTP code and the count reset simultaneously. For example:

- **OTP TTL**: 15 minutes
- **Count TTL**: 15 minutes

This way, a user cannot wait for the count to reset and try more attempts, as the OTP code would have expired at the same time.

Create account									
Action	**ID**	**Current business rule**	**Updated business rule**	**Date modified**	**HMRC requirement**	**Lockout**	**Security rationale for either:** Extending lockout to 2 hours, staying as 15 minutes or no lockout	**OTP TTL**	Count TTL

Entered incorrect SMS code 6x		The user has 5 attempts to enter the code correctly. The 6th incorrect attempt = locked out for 15 minutes	No change from the as-is		N/A	Y- 15 mins	It could be used to send messages to another mobile number - spam - reputational damage, but easier to do it through create. Each OTP should only allow 5 attempts to get the correct value before a new OTP needs to be issued. This is to prevent brute force attacks. The number of OTP requested needs to be limited.	15 minutes	15 minutes
Entered incorrect email code 6x		user has 5 attempts to enter the code. after 6th incorrect attempt, they must get a new code and try again. No lockout is applied.	No change from the as-is		N/A	N		1 hour	1 hour
Entered incorrect Auth app code 6x		The user has unlimited attempts at entering the OTP code from their AA correctly.	No change from the as-is		N/A	N	Not sure on security risk. Each OTP should only allow 5 attempts to get the correct value before a new OTP needs to be issued. This is to prevent brute force attacks. The number of OTP requested needs to be limited.	120 seconds*	15 minutes
Requested SMS code 6x		A user can request for an SMS OTP Code 5 times. On the 6th time they are blocked	A user can request for an SMS OTP Code 5 times. On the 6th time they are	02.05.24	AUT-2377	Y- 2hrs	**Discouraging Automated Attacks:** Automated scripts or bots are often used to carry out attacks by making a large number of login attempts in a short period. A longer lockout period frustrates these automated attempts, as they are forced to wait for an extended duration between each trial. The purpose of this stage in the journey	15 minutes	15 minutes

		for 15 minutes.	blocked for 2 hours				is to validate that the user owns the mobile device, which means we are sending an SMS to any number that is entered. This could be 'spammed' sending lots of SMS to victims mobile phones in the name of GOVUK causing reputational damage. Protect against DDOS on GOV.UK Notify Protect against malicious actors requesting SMS to premium rate and exploit		
Requested Email code 6x		User requests email OTP code 6 times and is locked out for 15 minutes.	User requests email OTP code 6 times and is locked out for 2 hours.	02.05.24	CREATE AUT-2445	Y-2hrs		1 hour	1 hour

Sign in

Journey	ID	Business rule	Updated business rule	Date modified	HMRC requirement	Lockout	Security rationale for lockout	OTP TTL	Count TTL
Entered incorrect SMS code 6x		After 6 incorrect attempts, the user will be locked out for 15 minutes	After 6 incorrect attempts, the user will be locked out for 2hours	02.05.24	AUT-2064	Y - 2hrs	Reduces an attackers ability / time taken to brute force attack the SMS OTP. Discourage automated attacks Reduce impact of stolen credentials.	15 minutes	15 minutes
Entered incorrect Auth app code 6x		After 6 incorrect attempts, the user will be locked out for 15 minutes	After 6 incorrect attempts, the user will be locked out for 2hours	02.05.24	AUT-2061	Y - 2hrs	Reduces an attackers ability / time taken to brute force attack the Authenticator app request, this can be a bigger issue than SMS as a number of OTP numbers can be valid at one time.	150 seconds	15 minutes

Entered incorrect password 6x		After 6 incorrect attempts, the user will be locked out for 15 minutes	After 6 incorrect attempts, the user will be locked out for 2hours	02.05.24	AUT-2060	Y - 2hrs	**Mitigating brute force attacks**: Increasing the lockout period makes it more challenging for attackers to perform brute force attacks. A longer lockout period reduces the number of attempts an attacker can make within a given time frame, making it more difficult to guess the correct password **Discouraging Automated Attacks**: Automated scripts or bots are often used to carry out attacks by making a large number of login attempts in a short period. A longer lockout period frustrates these automated attempts, as they are forced to wait for an extended duration between each trial.		2 hours
Requested SMS code 6x		After 6 requests of an SMS code, the user will be locked out for 15 minutes	After 6 incorrect attempts, the user will be locked out for 2hours	02.05.24	AUT-2378	Y - 2hrs	**Discouraging Automated Attacks:** Automated scripts or bots are often used to carry out attacks by making a large number of login attempts in a short period. A longer lockout period frustrates these automated attempts, as they are forced to wait for an extended duration between each trial. The purpose of this stage in the journey is to validate that the user owns the mobile device, which means we are sending an SMS to any number that is entered. This could be 'spammed' sending lots of SMS to victims mobile phones in the name of GOVUK causing reputational damage. Protect against DDOS on GOV.UK Notify Protect against malciious actors requesting SMS to premium rate and explout		

Password reset

Journey	**ID**	**Business Rule**	**Updated business rule**	**Date mo**	**HMRC requ**	**Lockout**	**Security rationale**	**OTP TTL**	Count TTL

				dified	irement				
Entered incorrect SMS code 6x		Entering an SMS code was not previously part of the password reest journey, therefore no lockout rule exist	After 6 incorrect attempts, the user will be locked out for 2 hours	02.05.24	AUT-2070	Y - 2hrs	Reduces an attackers ability / time taken to brute force attack the SMS OTP. Discourage automated attacks Reduce impact of stolen credentials.	15 minutes	15 minutes
Entered incorrect email code 6x		After 6 incorrect attempts, the user will be locked out for 15 minutes	After 6 incorrect attempts, the user will be locked out for 2 hours	02.05.24	AUT-2071	Y - 2hrs	Each OTP should only allow 5 attempts to get the correct value before a new OTP needs to be issued. This is to prevent brute force attacks. The number of OTP requested needs to be limited.	15 minutes	15 minute
Entered incorrect Auth 6x		Entering an SMS code was not previously part of the password reest journey, therefore no lockout rule exist	After 6 incorrect attempts, the user will be locked out for 2 hours	02.05.24	AUT-2072	Y	**Discouraging Automated Attacks:** Automated scripts or bots are often used to carry out attacks by making a large number of login attempts in a short period. A longer lockout period frustrates these automated attempts, as they are forced to wait for an extended duration between each trial.	150 seconds	15 minutes

Requested SMS code 6x		Entering an SMS code was not previously part of the password reest journey, therefore no lockout rule exist	After 6 requests of an SMS code, the user will be locked out for 2 hours	02.05.24	AUT-2379	Y	**Discouraging Automated Attacks:** Automated scripts or bots are often used to carry out attacks by making a large number of login attempts in a short period. A longer lockout period frustrates these automated attempts, as they are forced to wait for an extended duration between each trial. The purpose of this stage in the journey is to validate that the user owns the mobile device, which means we are sending an SMS to any number that is entered. This could be 'spammed' sending lots of SMS to victims mobile phones in the name of GOVUK causing reputational damage. Protect against DDOS on GOV.UK Notify Protect against malciious actors requesting SMS to premium rate and explout	15 minutes	15 minutes
Requested email code 6x		1. user will be blocked for 15 minutes if they request a new email OTP code more than 5 times (6th request = block)	After 6 requests of an SMS code, the user will be locked out for 2 hours	02.05.24	AUT-2381	Y	**Discouraging Automated Attacks:** Automated scripts or bots are often used to carry out attacks by making a large number of login attempts in a short period. A longer lockout period frustrates these automated attempts, as they are forced to wait for an extended duration between each trial. **Reputational damage** The purpose of this stage in the journey is to validate that the user owns the email account, which means we are sending an email to any email address that is entered. This could be 'spammed' sending lots of emails to victims email account in the name of GOVUK causing reputational damage.	15 minutes	15 minutes

MFA Account recovery

Journey	ID	Business rule	Updated business rule	Date modified / go live	HMRC requirement	Lockout	Security rationale	OTP TTL	Count TTL
Requested email code 6x		A user will be blocked for 15 minutes if they request a new email OTP code more than 5 times (6th request = block)	A user will be blocked for 2 hours if they request a new email OTP code 6x	02.05.24	AUT-2382	Y-2hrs	**Discouraging Automated Attacks:** Automated scripts or bots are often used to carry out attacks by making a large number of login attempts in a short period. A longer lockout period frustrates these automated attempts, as they are forced to wait for an extended duration between each trial. **Reputational damage** The purpose of this stage in the journey is to validate that the user owns the email account, which means we are sending an email to any email address that is entered. This could be 'spammed' sending lots of emails to victims email account in the name of GOVUK causing reputational damage.		
Requested SMS code 6x			A user will be blocked for 2 hours if they request a new SMS code 6x	02.05.24	AUT-2380	Y-2hrs	**Discouraging Automated Attacks:** Automated scripts or bots are often used to carry out attacks by making a large number of login attempts in a short period. A longer lockout period frustrates these automated attempts, as they are forced to wait for an extended duration between each trial. The purpose of this stage in the journey is to validate that the user owns the mobile device, which means we are sending an SMS to any number that is entered. This could be 'spammed' sending lots of SMS to victims mobile phones in the name of GOVUK causing reputational damage. Protect against DDOS on GOV.UK Notify		

							Protect against malciious actors requesting SMS to premium rate and explout		
Entered incorrect SMS 6x		A user has 6 attempts to enter the SMS code correctly. After this, they will be sent to a new code. there will be a 15 minute block for users who enter the OTP code incorrect 6x	No change		AUT-2082	Y-15 mins	Lockout not effective as In an attack scenario the account has already been compromised and is now in control of the attacker. They would then set up a device that they control as 2FA. It could be used to send messages to another mobile number - spam - reputational damage, but easier to do it through create. Each OTP should only allow 5 attempts to get the correct value before a new OTP needs to be issued. This is to prevent brute force attacks. The number of OTP requested needs to be limited.	**15 minutes**	15 minutes
Entered incorrect auth app code 6x		No lockout	No lockout	02.05.24	AUT-2135		Lockout not effective as In an attack scenario the account has already been compromised and is now in control of the attacker. They would then set up a device that they control as 2FA. Each OTP should only allow 5 attempts to get the correct value before a new OTP needs to be issued. This is to prevent brute force attacks. The number of OTP requested needs to be limited.	**150 seconds**	15 minutes

TTL for Re-authentication

Journey	OTP TTL	to be OTP TTL	Count TTL	to be Count TTL
Email entry	N/A	N/A	15 mins	2 hours
Password entry	N/A	N/A	15 mins	2 hours

Auth app security code	150 seconds		15 minutes	15 minutes*
SMS code	15 mins		15 mins	15 minutes*

Re-authentication rules

Re-authentication									
Journey	**ID**	**V1 Business rule**	**Date modified**	**V2 Business rules**	**Date modified**	**HMRC requirement**	**Security rationale for logout not lockout**	**OTP TTL**	**Count TTL**
Entered incorrect SMS code 6x		After 6 incorrect attempts, the user will be **locked out for 2hours**	16.04.24	After 6 incorrect attempts, the user will be **logged out** not locked out	02.07.24				
Entered incorrect email address 6x		After 6 incorrect attempts, the user will be **locked out for 2hours**	16.04.24	After 6 incorrect attempts, the user will be **logged out** not locked out	02.07.24				
Entered incorrect Auth app code 6x		After 6 incorrect attempts, the user will be **locked out for 2hours**	16.04.24	After 6 incorrect attempts, the user will be **logged out** not locked out	02.07.24				
Entered incorrect		After 6 incorrect attempts, the user	16.04.24	After 6 incorrect attempts, the user	02.07.24				

password 6x		will be locked out for 2hours		will be logged out not locked out					
Requested SMS code 6x		After 6 incorrect attempts, the user will be locked out for 2hours	16.04.24	After 6 incorrect attempts, the user will be logged out not locked out	02.07.24				

Account management rules

Users also receive OTP codes during certain account management journeys. These journeys are accessed via the account management relying party (known as the user’s One Login Home) which requires 2-factor authentication for the user to access it. When a user is signed in they are additionally challenged to enter their password before they can begin any journey that involves adding or updating sign in information.

Account management

Journey	Business rule	Updated business rule	Date modified	HMRC requirement	Lock out	Security rationale	OTP TTL	Count TTL
Update email address - the user must enter an email address OTP sent to their new email address	There is no limit on the number of times a user may enter an incorrect email verification OTP code or request a new one	N/A	N/A	No specific requirement about this	No	A user must authenticate with 2 factors in order to access their account management area and begin this journey. The user must additionally provide their password in order to begin the update email address journey. These controls provide sufficient confidence that the user is the genuine owner of the account not to enforce any limits on the number of times they may enter a code.	15 minutes	N/A - no count

Update phone number - the user must enter an SMS OTP sent to their new phone number	There is no limit on the number of times a user may enter an incorrect SMS OTP code or request a new one	N/A	N/A	No specific requirement about this	No	A user must authenticate with 2 factors in order to access their account management area and begin this journey. The user must additionally provide their password in order to begin the update phone number journey. These controls provide sufficient confidence that the user is the genuine owner of the account not to enforce any limits on the number of times they may enter a code.	15 minutes	N/A - no count
[under development] Add new phone number - the user must enter an SMS OTP sent to their new phone number	There is no limit on the number of times a user may enter an incorrect SMS OTP code or request a new one	N/A	N/A	No specific requirement about this	No	A user must authenticate with 2 factors in order to access their account management area and begin this journey. The user must additionally provide their password in order to begin the add phone number journey. These controls provide sufficient confidence that the user is the genuine owner of the account not to enforce any limits on the number of times they may enter a code.	15 minutes	N/A - no count
[under development] Add authenticator app - the user must enter a TOTP generated by their new	There is no limit on the number of times a user may enter an incorrect authenticator app TOTP	N/A	N/A	No specific requirement about this	No	A user must authenticate with 2 factors in order to access their account management area and begin this journey. The user must additionally provide their password in order to begin the add authenticator app journey. These controls provide sufficient confidence that the user is the genuine	Approximately 5 minutes - the user's authenticator app will generate a code every 30 seconds and One	N/A - no count

authenticator app						owner of the account not to enforce any limits on the number of times they may enter a code.	Login will accept codes generated up to 2.5 minutes of the time at which the MFA challenge was issued AUT-3432: How long is our MFA code verification window? DONE	
[under development] Update authenticator app - the user must enter a TOTP generated by their new authenticator app	There is no limit on the number of times a user may enter an incorrect authenticator app TOTP	N/A	N/A	No specific requirement about this	No	A user must authenticate with 2 factors in order to access their account management area and begin this journey. The user must additionally provide their password in order to begin the update authenticator app journey. These controls provide sufficient confidence that the user is the genuine owner of the account not to enforce any limits on the number of times they may enter a code.	Approximately 5 minutes - the user’s authenticator app will generate a code every 30 seconds and One Login will accept codes generated up to 2.5 minutes	N/A - no count

							before or after the time at which the MFA challenge was issued AUT-3432: How long is our MFA code verification window? DONE	

Back-up MFA method

Journey	Business rule	Updated business rule	Lock out	Security rationale	OTP TTL	Count TTL	
Entered incorrect SMS code 6x (Prompt at create and sign in journeys)	A user has 5 attempts to enter the code correctly when adding an auth app or a mobile number as back-up MFA method, during a create / sign-in journey. At the 6th incorrect	N/A	No	As the user has already been authenticated via the default MFA method, there’s no justification to lock a user out if they fail to enter the correct security code when setting up a back-up MFA method.	15 minutes	I5 minutes	

	attempt, the user will be shown a message stating that they will not be able to add a back-up method now but can do so another time. No lockout will be enforced on the user.						
Requested to send SMS code 6x not (Prompt at create and sign in journeys)	A user has 5 attempts to request security code when adding a mobile number as back-up MFA method, during a create / sign-in journey. At the 6th request, the user will be shown a message stating that they will not be able to add a back-up method now but can do so another time.	N/A	No	As the user has already been authenticated via the default MFA method, there's no justification to lock a user out if they fail to enter the correct security code when setting up a back-up MFA method.	15 minutes	15 minutes	

	No lockout will be enforced on the user.						
Sign in journey (back-up method added) - Entered incorrect SMS code 6x	Given a user has selected their back up MFA method during a sign-in journey, after 6 incorrect attempts, the user will be locked out for 2 hours (Auth app and SMS)	N/A	Yes - 2 hours	This will be in line with existing business rule for default MFA method	150 seconds - Auth App 15 minutes - SMS	15 minutes	
Sign in journey (back-up method added) - Request security code 6x	A user can request for an SMS OTP Code 5 times if they've chosen their back-up MFA method for authentication. On the 6th time they are blocked for 2 hours	N/A	Yes - 2 hours	This will be in line with existing business rule for default MFA method	15 minutes	15 minutes	
Prompt during MFA reset - entering code	A user has 5 attempts to enter the code correctly when adding an auth app or a mobile number as back-up MFA method, during an MFA reset	N/A	No	As the user has already been authenticated via the default MFA method, there's no justification to lock a user out if they fail to enter the correct security code when setting up a back-up MFA method.	150 seconds - Auth App 15 minutes - SMS	15 minutes	

	journey. At the 6th incorrect attempt, the user will be shown a message stating that they will not be able to add a back-up method now but can do so another time. No lockout will be enforced on the user.						
Prompt during MFA reset - requesting code	A user has 5 attempts to request security code when adding a mobile number as back-up MFA method, during an MFA reset journey. At the 6th request, the user will be shown a message stating that they will not be able to add a back-up method now but can	N/A	No	As the user has already been authenticated via the default MFA method, there’s no justification to lock a user out if they fail to enter the correct security code when setting up a back-up MFA method.	15 minutes	15 minutes	

	do so another time. No lockout will be enforced on the user.						
Choosing back-up MFA method during MFA reset (Entered incorrect code 6x)	Given a user has selected their back up MFA method during MFA reset journey, after 6 incorrect attempts, the user will be locked out for 2 hours (Auth app and SMS)	N/A	Yes - 2 hours	This will be in line with existing business rule for default MFA method	150 seconds - Auth App 15 minutes - SMS	15 minutes	
Choosing back-up MFA method during MFA reset (Requested SMS code 6x)	A user can request for an SMS OTP Code 5 times if they've chosen their back-up MFA method for authentication. On the 6th time they are blocked for 2 hours	N/A	Yes - 2 hours	This will be in line with existing business rule for default MFA method			
Choosing back-up MFA method during Password reset journey (Entered incorrect code 6x)	After 6 incorrect attempts, the user will be locked out for 2 hours if they've selected their back-up MFA	N/A	Yes - 2 hours	This will be in line with existing business rule for default MFA method	150 seconds - Auth App 15 minutes - SMS	15 minutes	

	method for authentication. (Auth app and SMS)						
Choosing back-up MFA method during Password reset journey (Requested SMS code 6x)	A user can request for an SMS OTP Code 5 times if they’ve chosen their back-up MFA method for authentication. On the 6th time they are blocked for 2 hours	N/A	Yes - 2 hours	This will be in line with existing business rule for default MFA method	15 minutes	15 minutes	
Choosing back-up MFA method during Reauth journey (Entered incorrect code 6x)	After 6 incorrect attempts, the user will be locked out for 2 hours if they’ve selected their back-up MFA method for authentication. (Auth app and SMS)	N/A	Yes - 2 hours	This will be in line with existing business rule for default MFA method			
Choosing back-up MFA method during Reauth journey (Requested SMS code 6x)	A user can request for an SMS OTP Code 5 times if they’ve chosen their back-up MFA method for authentication. On the 6th time they are blocked for 2 hours	N/A	Yes - 2 hours	This will be in line with existing business rule for default MFA method			

Choosing back-up MFA method during Uplift journey (Entered incorrect code 6x)	After 6 incorrect attempts, the user will be locked out for 2 hours if they’ve selected their back-up MFA method for authentication. (Auth app and SMS)	N/A	Yes - 2 hours	This will be in line with existing business rule for default MFA method	150 seconds - Auth App 15 minutes - SMS	15 minutes	
Choosing back-up MFA method during Uplift journey (Requested SMS code 6x)	A user can request for an SMS OTP Code 5 times if they’ve chosen their back-up MFA method for authentication. On the 6th time they are blocked for 2 hours	N/A	Yes - 2 hours	This will be in line with existing business rule for default MFA method	15 minutes	15 minutes	