Responsible Vulnerability Disclosure Policy

This is the **Lloyds Banking Group ("LBG")** Responsible Vulnerability Disclosure Policy (the "Policy").

You must read this Policy in full before you attempt to access any LBG systems or report any vulnerabilities, and comply with it at all times.

The safety and security of all our data, including our customer and colleague data, and the reliability of our products and services, are of the paramount importance to **LBG**. This Policy is intended to guide security researchers on how to share any identified issues with **LBG** in a responsible way.

This Policy provides a framework that allows for the safe, secure, and responsible disclosure of weaknesses in our information technology infrastructure which can be exploited to perform unauthorised actions within LBG systems ("vulnerabilities"). The purpose of this Policy is to enable vulnerabilities to be reported in a timely and responsible manner, and facilitating remediation to retain the integrity, continuity, and security of LBG services.

LBG endorse and support working with the research and security practitioner community to improve our online security.

LBG are committed to:

- Investigating and resolving security issues in our platform and services thoroughly
- Working in collaboration with the security community
- Responding promptly and actively to valid and in scope matters identified

This Policy explains how **LBG** works with the security research community to improve our online security.

Note that:

- ***Parties are required to always act in compliance with all laws and regulations and this Policy.***
- This Policy does not provide the security researcher any form of indemnity from LBG or third party for any actions in breach of the law or of this Policy.
- The security researcher is not acting on LBG's behalf (whether as an agent, employee, partnership or through any joint venture arrangement.
- The security researcher is not authorised to access personal data.

The process described herein is not intended for submitting complaints about LBG services or products, reporting issues with bank accounts, card fraud, ATMs, malware or asking questions about the availability of LBG websites or mobile banking services.

Confidentiality & Data Protection

You must treat all information about our systems, staff or customers that comes into your possession or that you otherwise become aware of, which is not publicly available, as strictly confidential, and not share or otherwise use it for any purpose other than emailing it to us as a submission as described above.

If you inadvertently access personal data on an LBG system you must immediately stop accessing the data, report this to LBG and follow all further instructions from LBG. You must follow data protection laws when reporting a vulnerability.

1. Scope

Vulnerabilities in our software or environments which threaten the confidentiality, integrity or availability of our systems, services, data, or our customers' data. Typical vulnerabilities accepted include OWASP Top 10 vulnerability categories and other vulnerabilities with demonstrated impact.

To be acknowledged in accordance with section 3 below, vulnerabilities must be original and previously unreported, and otherwise comply with this Policy.

Sites: All LBG owned services and sites are in scope.

You agree not to disclose vulnerability details to anyone other than LBG without LBG's written permission.

Out of scope

Any activity listed below or other activity that in any way breaches any law, regulation, court order, official guidance in any jurisdiction, or is otherwise contrary to this Policy, should not be undertaken.

This may include but is not limited to:

- Denial-of-Service attacks
- Brute forcing attacks.
- Physical or Social Engineering
- Putting exposed LBG data at risk.
- Uploading of any vulnerability or LBG related data to third-party utilities (e.g., Github, DropBox, YouTube)
- Do not "dive deeper" to determine how much more is accessible. If able to gain access to a system, accounts, users, or user data, stop at point of recognition and report.

We strongly discourage and will not respond to:

- Reports of generic vulnerabilities with no evidence of relevance to our systems
- Reports of any information already in the public domain
- Reports that are vague or non-actionable
- Vulnerabilities dependent upon social engineering techniques. For example, shoulder attack, stealing devices, phishing, fraud, stolen credentials or passwords.
- The submission of complaints, queries or reports not relevant to security vulnerabilities.

2. Requirements

General requirements:

- Please submit in the English language. Other languages may be supported but cannot be guaranteed.
- When documenting a vulnerability, if a vulnerability is public, please make sure any personal data is appropriately obfuscated in submission details.
- You agree that you are making your report without any expectation or requirement of reward or other benefit, financial or otherwise.
- We may modify the terms of this Policy or terminate the Policy at any time.
- You must report the vulnerability as soon as possible.
- All attack payload data must use professional language.

Must Nots:

- Jailbroken mobile devices must not be used to identify vulnerabilities. These will NOT be accepted and you may be reported to authorities for prosecution.
- On discovery of personal data (being any data relating to an identified or identifiable individual) or any data relating to LBG customers or colleagues, security researchers must immediately stop accessing the data, not download, move, alter or delete the data from the LBG system and report it to LBG and follow all instructions.
- Do not attempt to penetrate services and systems further than necessary to confirm the vulnerability finding.
- Do not pursue post-exploitation or pivot from the vulnerable target into other parts of the network.
- Credential Stuffing/Password Spraying attacks is prohibited.
- Do not access unnecessary amounts of data. For example, 2 or 3 records is enough to demonstrate most vulnerabilities, such as an enumeration or direct object reference vulnerability.
- Do not violate the privacy of the LBG customers, colleagues or third parties. Sharing, redistributing and/or not properly securing data retrieved from our systems or services, or similar activities is prohibited.
- Other than as described in section 3 below, do not communicate any vulnerabilities or associated details using methods not described in this Policy. This is not intended to stop you notifying a vulnerability to 3rd parties for whom the vulnerability is directly relevant e.g., where the vulnerability being reported is in a 3rd party software library or framework, however reference to LBG should not be contained within reports to 3rd parties.
- Do not modify data in LBG systems or services.
- Do not install your own backdoor in LBG systems to disclose the vulnerability as this may result in unnecessary damage and security risks.
- Do not copy, modify, or remove data from LBG systems. You may create a directory listing of the system.
- Do not negatively impact the confidentiality, integrity, or availability of LBG systems or services.
- Do not execute code on LBG systems.
- Do not disrupt LBG services or systems.
- You must not test the physical or electronic security of any property, building or presence of LBG, or LBG colleagues.

Credentials

If any credentials are discovered during recon and testing, these must be notified to us. The use of personal credentials for testing purposes is strictly prohibited and may trigger or result in investigations by the LBG fraud team and/or law enforcement. Please do not, under any circumstances, use credentials including your own personal account for testing purposes. This is to protect you and any/all of your own banking accounts/details. This Policy is set up as an unauthenticated initiative.

3. Reporting a vulnerability

If you have discovered something you believe to be an in-scope security vulnerability (see section 1 regarding scope), submit a report to the following email address: securitydisclosure@lloydsbanking.com

Your report should contain the following information:

Report Section	Description
Title	Concise summary categorising the vulnerability, and the site/application where it can be found E.g., Reflected XSS on the XYZ website
Asset	Web address, IP address, product, service name, etc
Weakness	Such as a CWE cwe.mitre.org
Severity	Such as low, medium, high, critical, and the calculated via CVSS score https://www.first.org/cvss/calculator/3.0
Description of the Vulnerability	• A summary of the vulnerability • Supporting files (e.g., screenshots, responses, logs, traces, or video) • Any mitigations or recommendations
Steps to reproduce	• Clear and descriptive steps to reproduce the vulnerability • Proof of concept code if available Proof of concept is the critical part of any vulnerability submission. Please provide clear, complete, and accurate reproducible steps that will allow LBG to validate the identified vulnerability as quickly as possible. This helps to ensure that the report can be triaged quickly and accurately whilst also reducing the likelihood of duplicate reports and/or malicious exploitation for some vulnerability classes (e.g., sub-domain takeovers).
Impact	The effects of successfully exploiting the vulnerability.
Contact details	• Name • Email Address (These details are optional to enable anonymous reporting)

You must not send your proof of exploit in the initial, plaintext email if the vulnerability is still exploitable. Please also ensure that all proof of exploits is in accordance with our guidance, if you are in any doubt, please email securitydisclosure@lloydsbanking.com for advice before sending the proof of exploit.

By Submitting a Report:

1. You consent to your information being stored by LBG and acknowledge you have read and accepted the terms of this Policy's guidelines.

2. You agree that any LBG information that you may encounter, view, acquire, or access, is owned by LBG or its customers, clients, or third-party providers. You have no rights, title, or ownership in any such information.

3. You agree that your research will be conducted for testing and research purposes only, and that you will not attempt to gain access to customer or user accounts or confidential information and will only interact with accounts you own.

4. You understand that nothing in this agreement, including submission of a report, shall be deemed to constitute the grant to you of any license or other right to or in respect of any LBG or third-party product, service, patent, trademark, trade secret, or other intellectual property.

5. By transmitting your submission to LBG, you perpetually allow us and our affiliates and subsidiaries the unconditional ability to use, modify, create derivative work from, distribute, disclose, and store information provided in your report or to have others do the same on our behalf, and these rights cannot be revoked. You present that the report is original to you and that you own all right, title, and interest in the submission.

6. You do not exploit or use in any manner the identified vulnerabilities or errors other than for the sole purpose of reporting it to LBG.

7. You will not engage howsoever with the intention of harming LBG, its customers, employees, partners or suppliers.

8. You will not use, misuse, delete, alter, or destroy, any data that you have accessed or may be able to access in relation to the vulnerability.

9. You agree to comply with instructions issued by LBG, including in relation to any data that you have accessed or stored.

What to expect:

LBG will treat submitted reports confidentially and will not share the finder's personal details with third parties without their authorisation, unless a disclosure is: required by law or legal process, in response to a lawful request from law enforcement, government agencies or other public bodies, or necessary or appropriate, as determined by LBG in its sole discretion, to protect our customers, our company, or our brands.

In response to your initial email, you will receive an acknowledgement email. All qualifying vulnerabilities will be investigated, and the submitter updated on progress at appropriate time.

4. Legal

This Policy is designed to be compatible with common vulnerability disclosure good practice. It does not give permission to act in any manner that is inconsistent with the law, or which might cause LBG to be in breach of any of its legal obligations, including but not limited to:

- The Computer Misuse Act (1990),
- The General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018,
- The Copyright, Designs and Patents Act (1988),
- The Official Secrets Act (1989),

or similar legislation, including laws or regulations enacted in other jurisdictions including (but not limited to) the US.

LBG affirms that it will not seek prosecution of any security researcher who reports any security vulnerability on a LBG service or system, where the researcher has acted in good faith and in accordance with this Policy.

Acknowledgements

LBG do not offer financial compensation. Where a vulnerability is verified, LBG will make efforts to show our appreciation to security researchers who take the time and effort to investigate and report security vulnerabilities to us, according to this Policy.