Title: Responsible Disclosure Program Terms

Description: Fanatics Betting & Gaming (FBG) takes information security seriously. That is why we are introducing our Responsible Disclosure Program! Your expertise can make a difference. If you are a cybersecurity enthusiast who's uncovered a vulnerability on any of our applications, websites, or systems ("FBG Properties"), we invite you to join our mission to keep data safe and protected. Our program provides a secure channel to report potential vulnerabilities. We provide these Terms to describe our philosophy regarding receipt of such disclosures as we work to validate and fix vulnerabilities in accordance with our commitment to protecting data and the FBG Properties.

Submitting a Responsible Disclosure Vulnerability Report

When reporting, we ask that you follow the following principles:

Be Thorough: Clearly describe the vulnerability, including steps to reproduce it. Provide as much detail as possible to help our team understand and verify the issue.

Stay Legal: Ensure your actions comply with applicable laws, regulations, and the Fanatics Sportsbook Terms of Service. Unauthorized access or actions that cause harm are strictly prohibited.

Focus on Security: Only report security vulnerabilities – such as remote code execution, data leaks, cross-site scripting (XSS), cross-site request forgery (XSRF), unauthorized access, etc. Do not report general bugs or non-security-related issues.

Provide Contact Information: Include your contact details so we can get in touch to acknowledge receipt and discuss the issue. We respect your privacy and will handle your information consistent with the commitments set forth in our Privacy Policy.

Exclusivity: Give us reasonable time to address the issue before disclosing it to others. We appreciate your patience while we work to fix the vulnerability.

Respect Confidentiality: Keep the details of the vulnerability confidential. Do not share the information with anyone else without our explicit permission.

Provide Proof of Concept: If possible, include a proof of concept (PoC) to demonstrate the vulnerability's impact. However, do not compromise user data or disrupt services in the process.

Be Responsive: Stay engaged throughout the resolution process. We may need additional information or clarifications to address the issue effectively.

In assessing vulnerabilities, do not:

- Access, acquire, remove, download, or modify data residing in an account that does not belong to you;
- Destroy or corrupt, or attempt to destroy or corrupt, data or information that does not belong to you;
- Execute or attempt to execute any “Denial of Service” attack;
- Post, transmit, upload, link to, send, or store any malicious software on the FBG Properties;
- Test in a manner that would result in the sending of unsolicited or unauthorized junk mail, spam, pyramid schemes, or other forms of duplicative or unsolicited messages or degrade the operation of any FBG Properties;
- Test third-party applications, websites, or services that integrate with or link to FBG Properties;
- Exploit any security vulnerability beyond the minimal amount of testing required to demonstrate that a potential vulnerability exists,

In sum, we ask that you refrain from harming or otherwise compromising FBG Properties, violating FBG Terms of Service, the rights of third parties or the law.

No Limitation of Liability to Third Parties

While FBG appreciates the reporting of potential vulnerabilities and does not intend to take action against individuals making good faith efforts to report such vulnerabilities lawfully and in compliance with these Terms, we are not able to make such a representation on behalf of third parties. Notably, to the extent that any security research or vulnerability disclosure activity involves the networks,

systems, information, applications, products, or services of any non-FBG entity, such non-FBG entity may independently determine whether to pursue legal action or remedies related to such activities.

Recognition

Your efforts contribute to a safer digital environment. Depending on the severity of the vulnerability, you may receive recognition or a token of appreciation from us.

Thank you for being a responsible security advocate. Your commitment to helping us improve the security of our systems is invaluable. Together, we make the digital world more secure for everyone.

Please email your submission to responsibledisclosure@betfanatics.com and we will reach out to you as soon as possible.

Thank you for helping FBG stay secure!