# FANDUEL'S LIAM SOMERVILLE ON PRIORITISING RESEARCHERS AS AN EXTENSION OF THE SECURITY TEAM

FANDUEL | hackerone

## The next time your friend of colleague goes on about their fantasy league, remember it's more than just a game. FanDuel, the web-based fantasy sports game with traditional season-long fantasy sports leagues compressed into daily or weekly games of skill, is used by over 8 million members across the globe.

With hundreds of millions of dollars being exchanged through weekly games, the small but mighty FanDuel security team is tasked with defending enormous amounts of sensitive data all while meeting rigorous state and national regulations.

**Liam Somerville**
Security Operations Engineer

FanDuel Security Specialist Liam Somerville says they see the security researcher community as an extension of their security team. Without the help from researchers, they couldn't be as secure as they are today. Over the course of their bug bounty program, FanDuel has resolved about 85 vulnerabilities and paid out over $35,000 in gratitude to researchers. We dove a little deeper with Liam to learn more about how his security team of seven works with the researcher community to boost security and how researchers can maximize their earnings by being creative. Take a look at our conversation.

**Q: Introduce yourself and FanDuel. Tell us what you do and why cybersecurity is so important to your business.**

**LS:** I'm Liam, I look after a small team in the Security Operations space here at FanDuel. We with HackerOne look after the bug bounty programme amongst other traditional security team functions.

Founded in 2009, FanDuel has redefined fantasy sports in pursuit of its mission of making sports more exciting. FanDuel offers a multitude of one-day, weekly and season-long game options for NFL, NBA, MLB, NHL, Golf, WNBA, and the EPL. Our one-day salary cap format gives you the flexibility to play on your own terms - when you want, for as much as you want - without having to commit to the entire season. Whether you play against your friends in a private league or in a public league, you can win cash, once-in-a-lifetime experiences or bragging rights, every night.

**Q: Why did FanDuel decide to start a bug bounty programme in the first place? What have been some results of your program to date?**

**LS:** The FanDuel product and its infrastructure is all developed in-house with a team of 150 engineers covering everything from devops, front end, backend, mobile, security and risk, among others. The entire security and risk team is currently made up of seven people...it was only two when I first started at the company. Currently there are only two security staff who spend part of their time with the bounty programme. With such a small team, it's impossible to have the time and the skills necessary to successfully do the monitoring and alerting of all our systems, vulnerability scanning, remediation, additional

projects, etc. Supplementing the testing with a bug bounty programme allows us to focus on other day to day activities that the security team is responsible for without adding large quantities of staff to the team. The HackerOne bug bounty program allows us to treat researchers as an extension of our team to further improve the security of the FanDuel platform for our customers. We simply can't do it without the help of researchers and, as a security team and as a company, we achieve far more, together, as one function.

Our bug bounty programme has been running since 2015 and, since then, we have accepted ~85 bugs and paid out more than $35,000 in bounties, with each of those researchers being added to the FanDuel Security Researcher Hall of Fame as an additional acknowledgement and thank you for their hard work.

**Q: What's the scope of your program? What findings are most interesting to your team?**

**LS:** We aim to have as wide of a scope as we possibly can, and we've included mobile apps, subdomains, a DNS name that we use internally so that if it ends up public and has a vulnerability, we still accept the bug report and reward the researcher. We've rewarded reports that are not listed as in scope, because we've seen it as an issue that we weren't comfortable with. While we have a defined scope, we're aware that "evil hackers", simply don't care about our scope or our risk appetite.

This said, though for some business and legal reasons we do have a small selection of "out of scope". All of our security staff and researchers are engineers, so it's really impressive seeing people join multiple vulnerabilities or technologies together to provide amazing proof of concepts. It's nice to stand back and just admire another person's work. We've even had several scenarios where the team really admired the proof of concept, the quality of the report, and the attitude of the researcher to the point we've received additional support from our CTO to double the bounties. To have the support of our management team to be able to do that is fantastic. Like hackers, we like breaking our own "rules" in favour of our researchers.

**Q: How does the bug bounty program impact your larger cybersecurity strategy?**

**LS:** FanDuel releases new code updates to production every day. Our team, and indeed an external pentest company simply is not going to be able keep up the way crowdsourced researchers can. This means we're not spending time having meetings regularly with pentest companies to scope and run tests. It allows us to dedicate that time saved on improving the security posture of our staff, implementing new technologies, working with our developers to improve the intricacies and defences of our product..

**Q: What results have you seen thus far? Anything surprising or unexpected?**

**LS:** Absolutely, we've had "we've done what?" moments, where we realised that, as a company, we got it wildly wrong. We've had moments where some of our best minds have wondered "why does that even work?". We've had reports that just stood out as being exceptionally well written, and we've even had one where the researcher provided a video where he talked through the issue, and how to create the PoC, and his thoughts of how to remediate it. It was really well made.

**Q: What has it been like working with hackers thus far? What has been one of your favorite hacker interactions to-date?**

**LS:** Honestly, it's been a really an interesting journey and great to work with such incredibly talented people.

I've loved getting to know some of the researchers personally through Twitter etc. It's a real community. Getting to hear about their personal lives, what they enjoy, what the find hard, hearing about family life, while seeing them excel and scoring big bounties.

**Q: What advice would you give hackers participating in your program?**

**LS:** It's important to remember that the team you're working with on the other side of the monitors may be really small and not in a position to reply quickly. They have other priorities as well as the bug bounty programme. We advise getting to know the team on the other side of the monitor personally. Remember, no one programme treats you the same way. I'm a researcher too, and I know the frustrations you face with programmes (they are mine too), but we are trying to minimise as much of that as possible on our programme. When we first launched with HackerOne we received ~200 reports in the first thirty days. How does a small team who have other daily responsibilities cope with that level of reports? The best we can. Don't get upset if you don't hear quickly, it's not personal. Most importantly YOU ARE VALUED! We can't strive to be a great security team without you! You are part of my team!

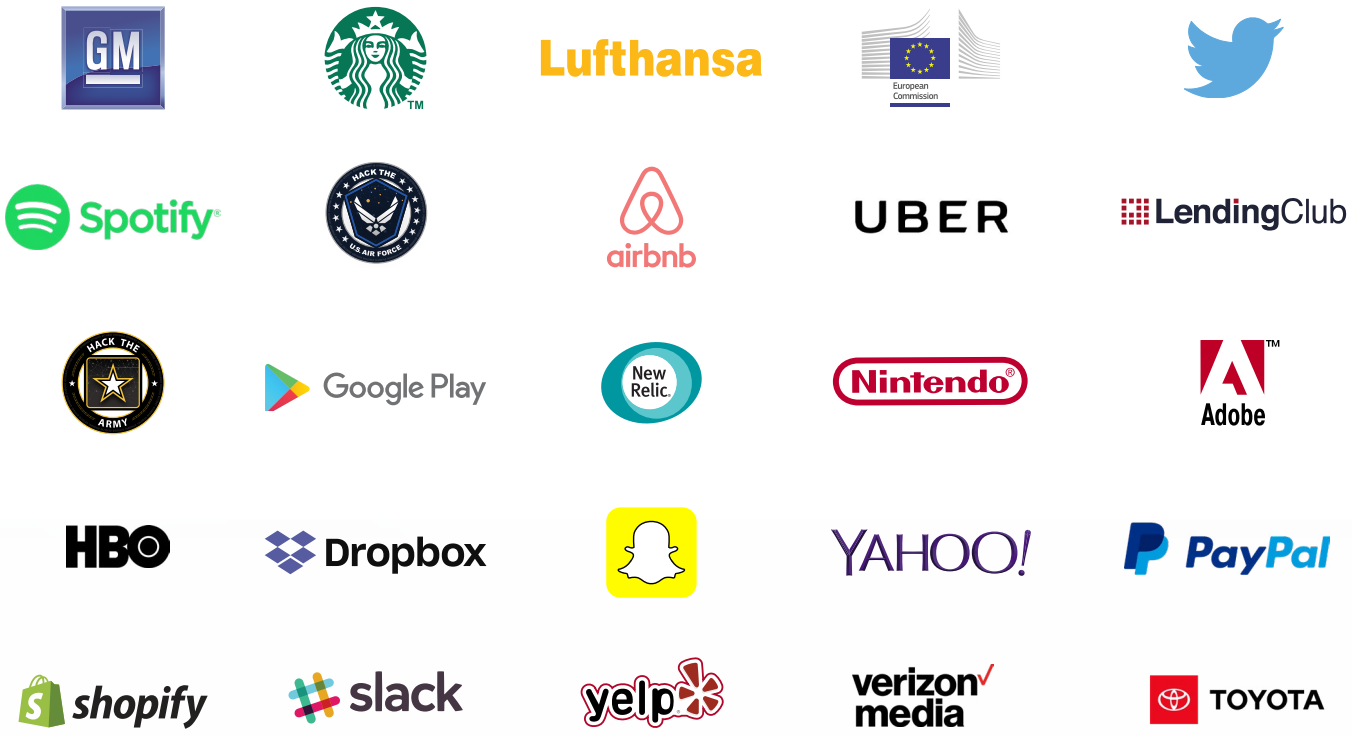
"We can't strive to be a great security team without you! You are part of my team!"

**LIAM SOMERVILLE,**
SECURITY OPERATIONS ENGINEER

---

If you're interested in learning more about FanDuel's program, check out the program page at https://hackerone.com/fanduel.

# HackerOne Has Vetted Hackers for Hundreds of Organizations Including:




# With Over 1,400 Organizations, More Companies Trust HackerOne Than Any Other Vendor

CONTACT US