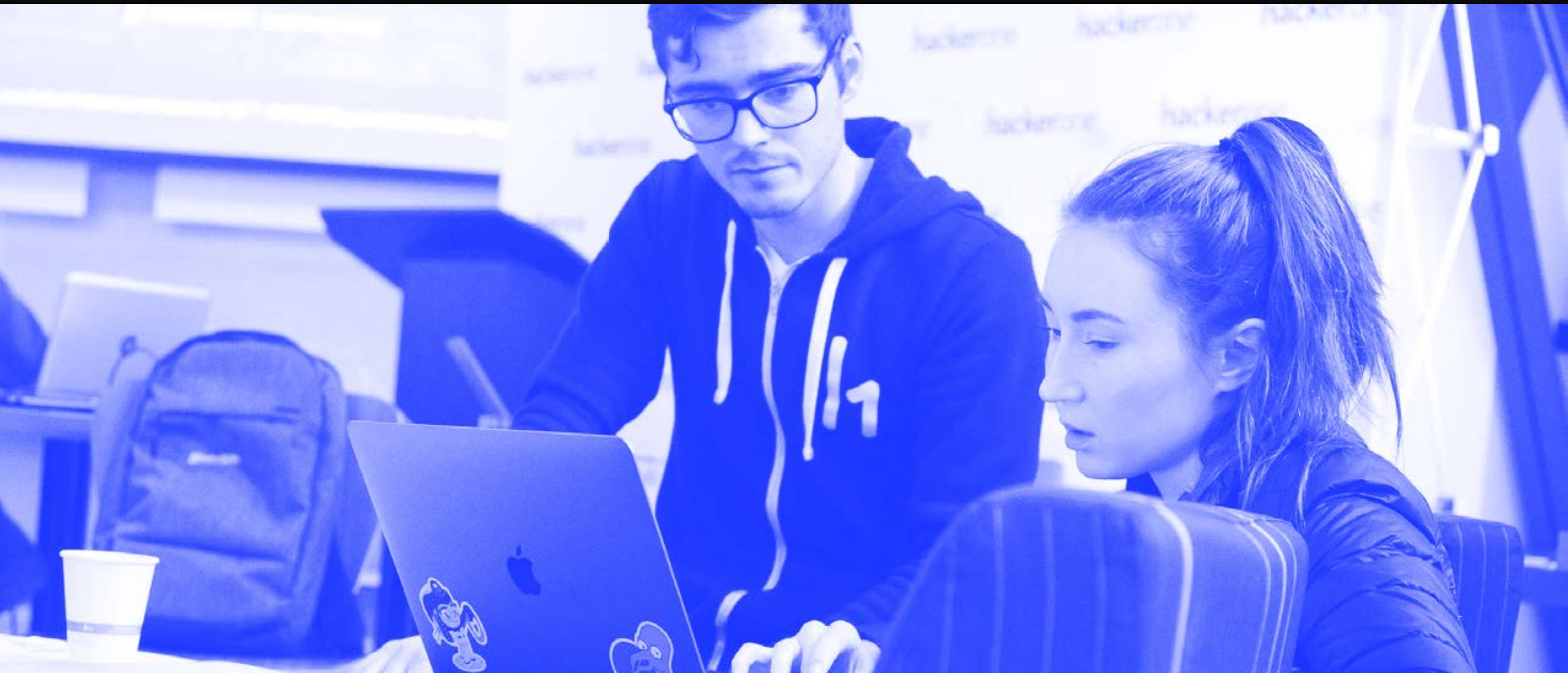
hackerone | STARLING BANK

CASE STUDY

Starling Bank Protects Customers' Funds with Hacker-Powered Security

Operating exclusively online, Starling Bank uses its own proprietary technology platform to power its banking services for more than 2.7 million personal and business accounts. In its continuous endeavour to ensure that customer funds are secure in the digital space, Starling Bank turned to HackerOne for support.



Key Takeaways

Before Challenges

- Looking for more resources to validate vulnerabilities and inform internal teams
- Wanted a streamlined process to remediate and validate reported risks by members of the public and 24/7 resources to help triage
- Looking for a flexible testing methodology to meet a range of security requirements and go beyond traditional pentesting
- Needed an extension of the internal team to scale faster and more effectively

Key Requirements

- GDPR adherence
- Representative demo environments for in-depth testing
- Structured reports to understand the broad attack surface, streamline submission flow, and implement quick and easy remediation
- 24/7 triage support to improve processes, meet SLA's, and enact transparent communication

Security Goals

- Move beyond traditional testing with a diverse bench of security research experts
- PII and financial security checks to ensure compliance with methodology-based testing
- Extend the internal team to scale and increase security coverage flexibly
- Verify best practices via a global community of research experts

Why HackerOne

- Most trusted and effective global community
- Run simple to complex workflows
- Scale cybersecurity processes
- Digital transformation enablement

Solutions

- HackerOne Response
- HackerOne Bounty
- HackerOne Triage
- HackerOne Advisory Services

Hacker Skill Sets

- Mobile Security Expertise
- Android and iOS Applications
- APIs and API Back-End
- OAuth and Developer Sandboxes

> **“We knew that to provide a secure digital experience for our customers, we needed a partner who could connect us with the diverse, global security researcher community, with a goal of identifying novel or unusual security issues on which traditional pentests don’t usually focus. So we decided to work with HackerOne.”**

Mark Rampton

HEAD OF CYBER SECURITY, STARLING BANK

About Starling Bank

Starling Bank was founded in 2014 and is an award-winning, fully licensed, and regulated bank built to give people a fairer, more intelligent, and more human alternative to the banks of the past. Starling Bank offers personal and business accounts alongside a range of other lending products. Starling also provides B2B banking and payments services through its Banking-as-a-Service model based on its proprietary technology platform. They were voted Best British Bank in 2018, 2019, 2020, and 2021.

Starling is a pioneer in the fast-growing challenger bank space, with a goal to help consumers simplify financial management using modern technology to bring banking into the present. Starling Bank offers services via mobile app and website, allowing customers to do all their banking digitally.

With more than two million customers banking online, and the personal identification information (PII) of those customers under their purview, Starling Bank's number one priority is to protect their customers' funds and data.

Full Coverage for an Evolving Attack Surface

Starling Bank's Head of Cyber Security, Mark Rampton, knows that if there is money to be made by compromising or exploiting a system, cybercriminals will take advantage. In the banking industry, vast amounts of consumer and financial data are entrusted to institutions for protection. Hypervigilance and advanced security planning are the best ways to stay ahead of threats. Mark is responsible for coordinating and running Starling Bank's offensive and defensive security teams. He also understands the hacker mindset. Before running security at Starling Bank, he was an ethical hacker for several consultancies.

Starling Bank operates exclusively as a digital platform. Starling is an online-only business, and its main cybersecurity goal is to protect its customers' funds and personal data while adhering to a security philosophy based on the "human firewall."

"If your instincts are telling you that something isn't quite right and you let the security team know, it goes a long way to getting visibility on the issue and tackling it, before it has the opportunity to negatively impact your customers," says Mark.

Starling Bank knew that running a dedicated Vulnerability Disclosure Program (VDP) could be resource-intensive. They also understood that an effective approach to cybersecurity takes a team effort. In 2019 they implemented a vulnerability disclosure policy via HackerOne Response. Their VDP created an easy way for the public to responsibly disclose vulnerabilities found in their applications and on their website. Starling Bank's security team wanted to work with the HackerOne community to see if they could find novel and unusual security issues that typical pentests don't usually find. They engaged with HackerOne to help bridge the gap between people and expertise and provide a platform to support interaction with the security researcher community.

"Finding the balance between security, usability, and functionality can be a challenge. We know that incorporating security early into internal processes goes a long way, but if you aren't working with every member of staff and understanding how they work and their needs, you'll still face hurdles," says Mark. "HackerOne complements our existing strategy by allowing us to approach security testing from multiple angles, from multiple independent parties, with varying levels of approach and scope."

At the beginning of the HackerOne partnership, Starling Bank wanted the security research community to focus on niche angles and look for bugs listed in the OWASP Top 10. These security researchers helped Starling Bank find classes of vulnerabilities that were often overlooked in standard penetration testing. By focusing on both niche areas and the most common vulnerabilities, the community findings led to Starling Bank writing automated tooling to seek out certain issues, which now sits in their testing stack. As a result of the automation and detection, Starling Bank has prevented certain security issues from appearing in their program, offering better protection to customers who are browsing or using the public-facing website.

> **"HackerOne complements our existing strategy by allowing us to approach security testing from multiple angles, from multiple independent parties, with varying levels of approach and scope."**
>
> **Mark Rampton**
> HEAD OF CYBER SECURITY,
> STARLING BANK

From Responsible Disclosure to Bug Bounty

After implementing HackerOne Response, Starling Bank met security researchers they would not have crossed paths with otherwise. After getting positive results from the responsible disclosure program, thanks to meaningful submission from the global community, Starling Bank decided to implement a private bug bounty program via HackerOne Bounty.

"We wanted to get the best of both worlds," says Mark. "We were excited to create an accessible VDP so any member of the public could take part and submit a report. Once we refined internal processes to accept and remediate vulnerabilities, we created a private bug bounty program to allow select security researchers to test some of our demo systems in-depth."

Starling bank provided a pre-production environment, and created an allow list to limit entry to approved security researchers. Operating within the demo environment ensured that live systems and data were not disrupted, and that hackers were able to test the newest features without disrupting each other.

By working directly with experienced hackers in these demo environments, and specifically with researchers with expertise in mobile security, Starling Bank gained a deeper understanding of where their assets could be vulnerable. As a result of findings submitted by the community, Starling Bank created several technical tools and initiatives that now provide increased visibility for identified issues. Automated tooling and new processes allow Starling Bank to ensure vulnerabilities found by security researchers are addressed in every planning and production cycle, so they are captured and resolved before being pushed to code. Starling Bank now builds greater internal awareness of vulnerabilities, which has led to the prevention of future issues.

Reducing Risk and Planning for Growth

Starling Bank also leverages HackerOne Triage and HackerOne Advisory Services as a way to support their internal team.

"HackerOne Services have been helpful for us to know that when a report is submitted, good quality reports rise to the top, and a quick response and turnaround is available to participants," explains Mark. "We hold ourselves accountable for meeting finance industry turnaround times so that our researchers' voice is recognized and issues are fixed in a prompt and timely manner."

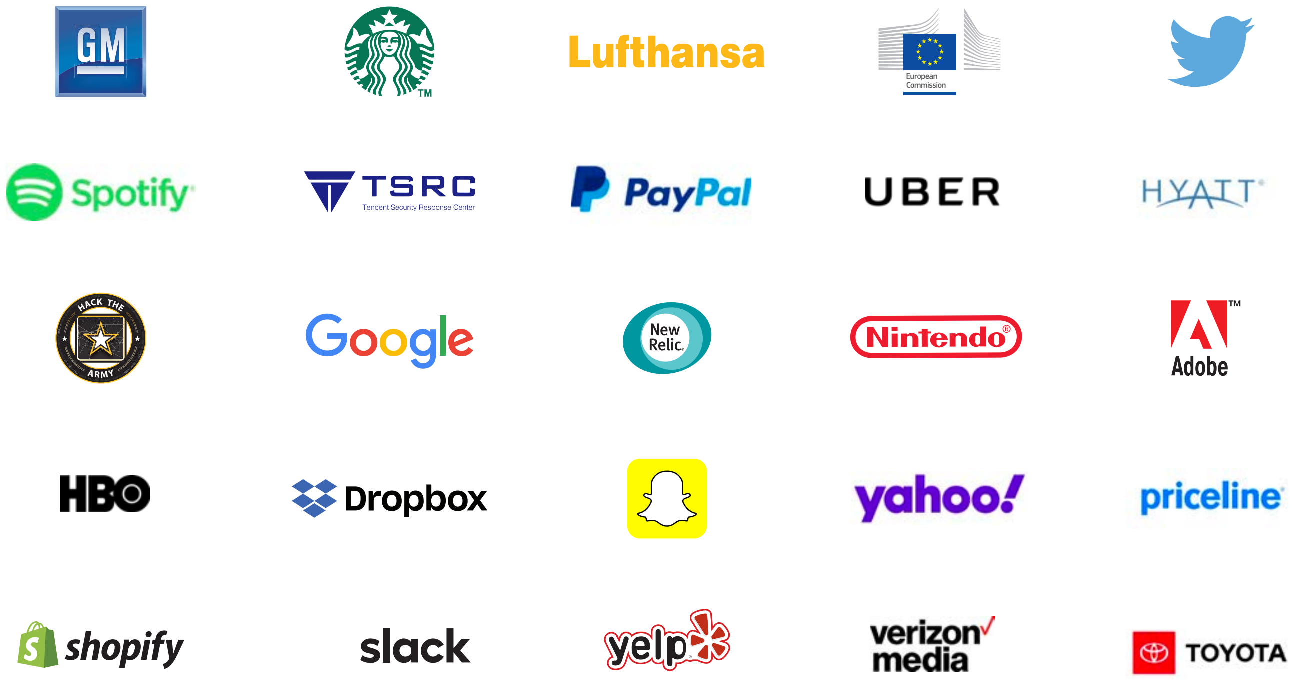
As Starling Bank looks to the future, they remain committed to recognizing, rewarding, and partnering with hackers worldwide, working toward a common goal of providing a secure environment for Starling Bank customers while recognizing and rewarding hard work from researchers who help them achieve that goal.

> **"HackerOne Services have been helpful for us to know that when a report is submitted, good quality reports rise to the top, and a quick response and turnaround is available to participants. We hold ourselves accountable for meeting finance industry turnaround times so that our researchers' voice is recognized and issues are fixed in a prompt and timely manner.""**

Mark Rampton
HEAD OF CYBER SECURITY,
STARLING BANK

hackerone

HackerOne has vetted hackers for hundreds of organizations including:



With over 2,000 customer programs, more companies trust HackerOne than any other vendor

Contact Us