# THE HACKER- POWERED SECURITY REPORT 2018

## FINANCIAL SERVICES & INSURANCE

hackerone

Vulnerability data and hacker-powered security adoption metrics for the financial services industry

# Executive Summary

The Hacker-Powered Security Report 2018 is the most comprehensive report on the bug bounty and vulnerability disclosure ecosystem. It contains a detailed analysis of 78,275 security vulnerability reports reported over the past year by ethical hackers through more than 1,000 programs on HackerOne.

**This report looks exclusively at the subset of those vulnerabilities and programs in the Financial Services & Insurance industry.**

Financial Services & Insurance organizations hold some of the most, if not *the* most, sensitive personal, financial, and other data. That said, it's reassuring to see the industry's adoption of hacker-powered security remains consistently in the top 4 of all industries.

While adoption of hacker-powered security is growing faster than ever, there is significant room for improvement. This is especially true in this industry, considering the potentially devastating impact—to individuals, organizations, and entire economies—any security breach could have.

By recognizing that criminals will discover vulnerabilities in nearly any software, application, or network surface they access, leaders must quickly and confidently shift their security strategy to an offensive approach, enabling them to beat criminals at their own game and reduce the risk of a serious security incident.

The time to act is now. Read this report to learn how leaders in the Financial Services & Insurance sector, such as Goldman Sachs and American Express, have prioritized hacker-powered security as an effective weapon against cyber risk.

> "Crowdsourced security testing is rapidly approaching critical mass, and ongoing adoption and uptake by buyers is expected to be rapid..."
>
> **GARTNER EMERGING TECHNOLOGY ANALYSIS:**
> *Bug Bounties and Crowdsourced Security Testing, June 2018*

# Contents

# Important Terms

**Hacker:** One who enjoys the intellectual challenge of creatively overcoming limitations.

**Hacker-Powered Security:** Any technique that utilizes the external hacker community to find unknown security vulnerabilities and reduce cyber risk. Common examples include private bug bounty programs, public bug bounty programs, time-bound bug bounty programs and vulnerability disclosure policies. With hacker-powered security testing, organizations can identify high-value bugs faster with help from the results-driven ethical hacker community.

**Hacktivity:** Hacker activity published on the HackerOne platform.

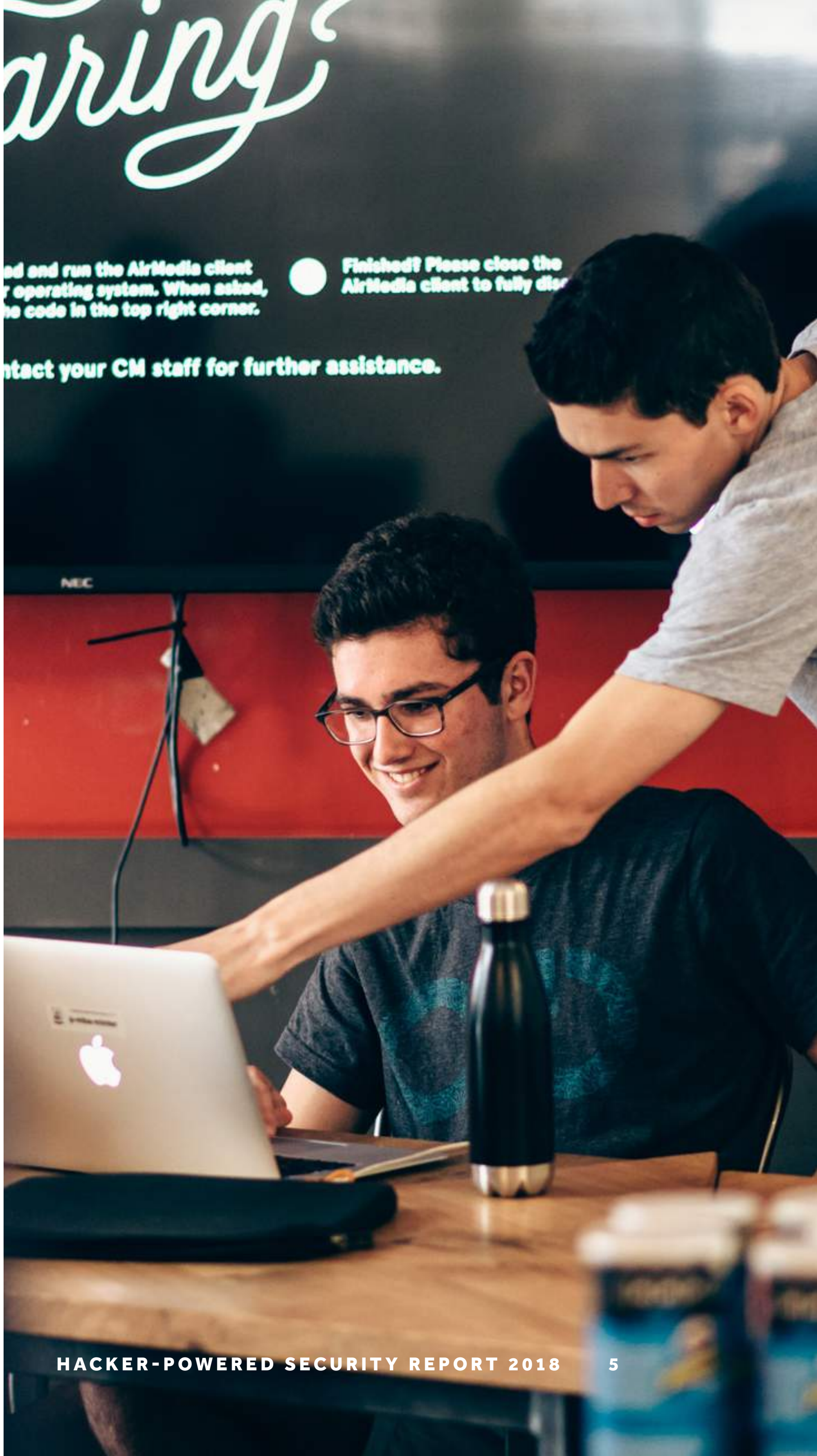
**Public Bug Bounty Program:** An open program any hackers can participate in for a chance at a bounty reward.

**Private Bug Bounty Program:** A limited access program that select hackers are invited to participate in for a chance at a bounty reward.

**Time-Bound Bug Bounty Challenge:** A program with a pre-determined limited time frame. In most cases hackers will register or be invited.

**Vulnerability:** Weakness of software, hardware, or online service that can be exploited.

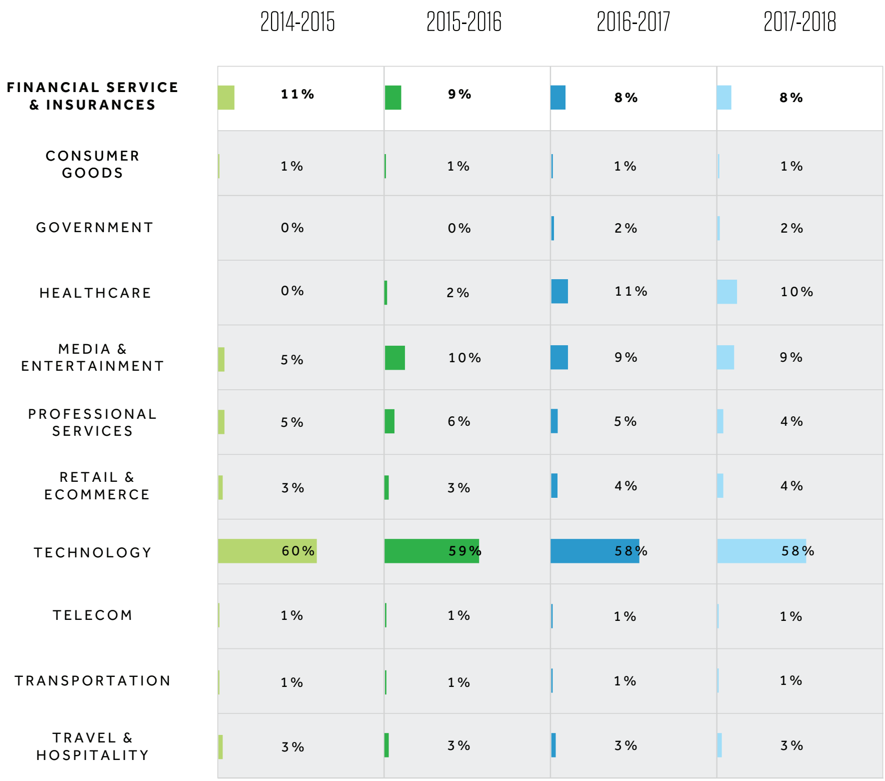
**Vulnerability Disclosure Policy (VDP):** An organization's formalized method for receiving vulnerability submissions from the outside world. This often takes the form of a "security@" email address. The practice is outlined in the Department of Justice (DoJ) Framework for a Vulnerability Disclosure Program for Online Systems and defined in ISO standard 29147.


aring
...d and run the AirMedia client
...r operating system. When asked,
...e code in the top right corner.
Finished? Please close the
AirMedia client to fully dis...
...tact your CM staff for further assistance.
NEC

# Key Findings

- **Financial Services & Insurance continues to adopt hacker-powered security.** With 8% of all new programs, the industry consistently ranks in the top four in adoption and far outpaces other industries, such as Government, Retail & Ecommerce, and Transportation.
- **Financial Services & Insurance pays low bounty amounts for critical bugs.** The average reward of $1,118 is nearly double the previous year, but is still less than one-third of the top industries. It also ranks at third from the bottom across all industries.
- **Financial Services & Insurance has the second-fastest average time to bug resolution.** This reflects a desire to fix bugs as soon as possible, quickly mitigating any potential risk. It also reflects a significant increase from the previous year, nearly cutting the average in half.
- **Financial Services & Insurance has the third-fastest average time to bounty payment.** At just 19 days, this industry pays hackers within days of the fastest industries and rewards them less than 3 weeks after a bug is first reported. This speed attracts more and better hackers, and is literally weeks faster than some other industries. It's also more than a week faster than the previous year's average.
- **The top bounty awarded by a Financial Services & Insurance organization is near the middle of the pack.** While it's difficult to compete with the tech industry's $75,000 top award, this industry's award is neither high nor low at $18,000. It did, however, nearly double year over year.
- **The Financial Services & Insurance industry has paid $1.4M in total bounties to date.** More than half that amount was paid out in the past year, an increase of 71% in just a single year.

**Percent Total Programs by Industry**



| | 2014-2015 | 2015-2016 | 2016-2017 | 2017-2018 |
|---|---|---|---|---|
| **FINANCIAL SERVICE & INSURANCES** | **11%** | **9%** | **8%** | **8%** |
| CONSUMER GOODS | 1% | 1% | 1% | 1% |
| GOVERNMENT | 0% | 0% | 2% | 2% |
| HEALTHCARE | 0% | 2% | 11% | 10% |
| MEDIA & ENTERTAINMENT | 5% | 10% | 9% | 9% |
| PROFESSIONAL SERVICES | 5% | 6% | 5% | 4% |
| RETAIL & ECOMMERCE | 3% | 3% | 4% | 4% |
| TECHNOLOGY | 60% | 59% | 58% | 58% |
| TELECOM | 1% | 1% | 1% | 1% |
| TRANSPORTATION | 1% | 1% | 1% | 1% |
| TRAVEL & HOSPITALITY | 3% | 3% | 3% | 3% |

**Figure 1:** *Industries that launched programs from the overall share of programs for that time period.*

# Bug Bounty Program Adoption by Industry

For the fourth year in a row, industries outside of Technology increased their share of the overall bug bounty market. While Technology companies still lead the pack, Financial Services & Insurance ranked fourth, accounting for 8% of all new programs launched.

Organizations like Goldman Sachs launched new programs, joining early Financial Services & Insurance adopters Local Tapiola, Coinbase, Lending Club, and others. The results from these programs and recommendations from government agencies demonstrate that hacker-powered security programs are a fast and reliable way to secure even the most sensitive digital data for some of the most risk-aware industries.

# Vulnerabilities by Industry

More than 78,000 vulnerabilities have been resolved on HackerOne as of May 2018, with more than one-third of those—27,000—resolved in the past year alone.

Taking a close look at the top 15 vulnerability types reported on HackerOne, cross-site scripting (XSS, CWE-79) continues to be the most common vulnerability across all industries, with the exception of Healthcare and Technology. For Financial Services & Insurance, 24% of all reported vulnerabilities fit this category.

Information Disclosure (CWE-200) accounted for 18% of the Financial Services & Insurance industry's reported vulnerabilities. The category covers instances when information is disclosed to an actor that is not explicitly authorized to have access to that information. This ranges from sensitive information within the product's own functionality—a private message, for example—to information about the product or its environment that is not normally available to an attacker, such as the installation path of a product that is remotely accessible.

# Vulnerabilities by Industry

| | FINANCIAL SERVICES & INSURANCE | CONSUMER GOODS | GOVERNMENT | HEALTHCARE | MEDIA & ENTERTAINMENT | PROFESSIONAL SERVICES | RETAIL & ECOMMERCE | TECHNOLOGY | TELECOM | TRANSPORTATION | TRAVEL & HOSPITALITY |
|---|---|---|---|---|---|---|---|---|---|---|---|
| CROSS-SITE SCRIPTING (XSS) | 24% | 23% | 26% | 19% | 28% | 27% | 24% | 21% | 24% | 59% | 38% |
| INFORMATION DISCLOSURE | 18% | 17% | 18% | 25% | 16% | 14% | 16% | 30% | 18% | 1% | 13% |
| IMPROPER AUTHENTICATION | 8% | 7% | 3% | 6% | 9% | 11% | 8% | 8% | 5% | 18% | 10% |
| VIOLATION OF SECURE DESIGN PRINCIPLES | 9% | 6% | 11% | 10% | 10% | 12% | 9% | 8% | 13% | 6% | 4% |
| CROSS-SITE REQUEST FORGERY (CSRF) | 10% | 12% | 4% | 8% | 7% | 5% | 12% | 7% | 8% | 2% | 8% |
| OPEN REDIRECT | 6% | 4% | 8% | 5% | 7% | 6% | 8% | 5% | 4% | 2% | 9% |
| PRIVILEGE ESCALATION | 4% | 5% | 1% | 1% | 3% | 5% | 5% | 5% | 10% | 3% | 6% |
| IMPROPER ACCESS CONTROL | 9% | 12% | 3% | 9% | 6% | 7% | 8% | 6% | 5% | 2% | 4% |
| CRYPTOGRAPHIC ISSUES | 2% | 2% | 18% | 1% | 2% | 2% | 1% | 2% | 3% | 1% | 1% |
| DENIAL OF SERVICE | 2% | 2% | 1% | 1% | 1% | 2% | 1% | 2% | 2% | 1% | 1% |
| BUSINESS LOGIC ERRORS | 5% | 4% | 1% | 4% | 5% | 6% | 4% | 4% | 3% | 2% | 5% |
| CODE INJECTION | 1% | 1% | 1% | 5% | 2% | 2% | 2% | 2% | 2% | 1% | 1% |
| SQL INJECTION | 1% | 5% | 5% | 4% | 2% | 0% | 2% | 2% | 2% | 2% | 1% |
| COMMAND INJECTION | 1% | 1% | 1% | 2% | 1% | 1% | 1% | 1% | 2% | 1% | 1% |
| MEMORY CORRUPTION | 1% | 1% | 0% | 0% | 1% | 0% | 1% | 1% | 1% | 1% | 0% |

**Figure 2:** *Listed are the top 15 vulnerability types platform wide, and the percentage of vulnerabilities received per industry.*

SPOTLIGHT

# Trusted Application Security for Blockchain and Cryptocurrency

As the use of cryptocurrency and other blockchain technologies explodes, the on-going security vetting by independent hackers is a must if these technologies are to prosper. In the fast-moving world of blockchain, only hacker-powered security has the breadth and deep bench to continuously maintain the same pace. The value is in the numbers. With a diverse community of hackers searching for security vulnerabilities around the clock, there is a much better chance of finding and fixing any potential weaknesses.

More than 40 of the top blockchain and cryptocurrency companies trust HackerOne and our community of ethical hackers to strengthen their security and protect their users. HackerOne has become the go-to hacker-powered security platform for companies with digital currencies or those built on blockchain technologies.

These companies have also structured their bounty programs to be attractive to hackers. Since these companies hold immense value, the bounties offered are correspondingly attractive. The largest bounty awarded to date was $11,000 for a cryptocurrency system vulnerability, and the largest potential award value is $200,000, offered by Augur.

coinbase

MONACO

COBINHOOD

electroneum

CoinMarketCap

MONERO

NANO

stellar

# Time to Resolution by Industry

Time to resolution is the number of business days it takes for a security team to resolve a reported bug. It's also a key indicator of program health and the primary metric that shows hackers what they can expect from a program. Security teams can also measure their own success by setting goals around average time to resolution for their program. With 27,000 valid reports resolved in 2017 on HackerOne alone, and 78,275 total reports submitted, facilitating this process from report to resolution is the primary role of HackerOne Services, which is used by many of our customers.

The best—in other words, fastest—industry with respect to average resolution times is Consumer Goods at 14 days. Close behind, however, is Financial Services & Insurance at just 19 days, followed by Healthcare (20 days). The industry with the slowest resolution time is Government (68 days).

There are a variety of reasons why resolution times vary from industry to industry, organization to organization. This can include complex technology stacks or supply chains that require coordination with partners and other vendors, as is typically the case for the relatively slow Telecommunications and Transportation organizations.

Once an issue is resolved, a bounty should be paid shortly thereafter—if not at the time of validation. This ensures not only hacker satisfaction, but that the organizational mechanisms for facilitating payment are aligned with the value provided by the hackers who identify the vulnerabilities.The industry with the fastest average days to bounty payment is, again, Healthcare at 15 days. Financial Services & Insurance is still one of the fastest industries at 19 days from report to bounty payment. On the other end of the spectrum, the industry with the most days to bounty payment is Travel & Hospitality (61 days).

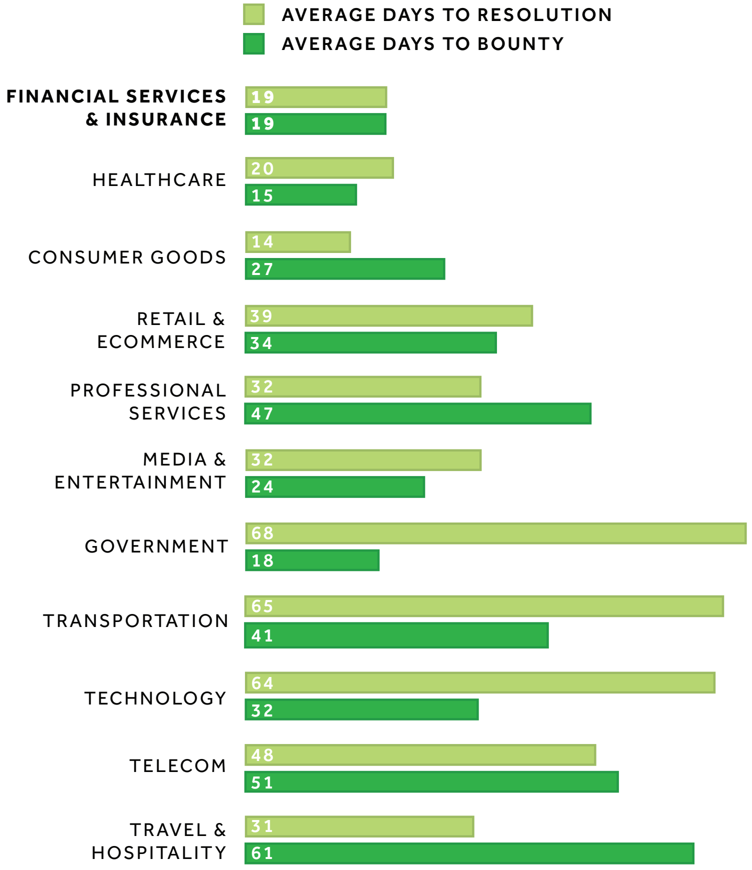


**Figure 3:** *Average number of days to resolution and to reward, measured from May, 2017 to April, 2018.*

# Financial Cybersecurity Statistics

## 8,500%

Detected cases of cryptojacking, which nefariously places "coinminers" on unsuspecting endpoint machines, increased by 8,500% in 2017.

Symantec

## 20%

In the Financial Services industry, "cyber risk management budgets can range anywhere from 5 percent to 20 percent of the total IT budget."

Deloitte

## 80%

"The number of cyber attacks against UK financial services companies reported to the UK's Financial Conduct Authority (FCA) has risen by more than 80% in the last year."

Information Age

## $225

"While the average cost to U.S. businesses per record lost or stolen in a breach was $225 across all industries in 2017, the cost per record for businesses in the financial industry was $336."

Generali

## 40

"Failures in cybersecurity have prompted data privacy legislation in more than 40 US states."

PwC

## 130%

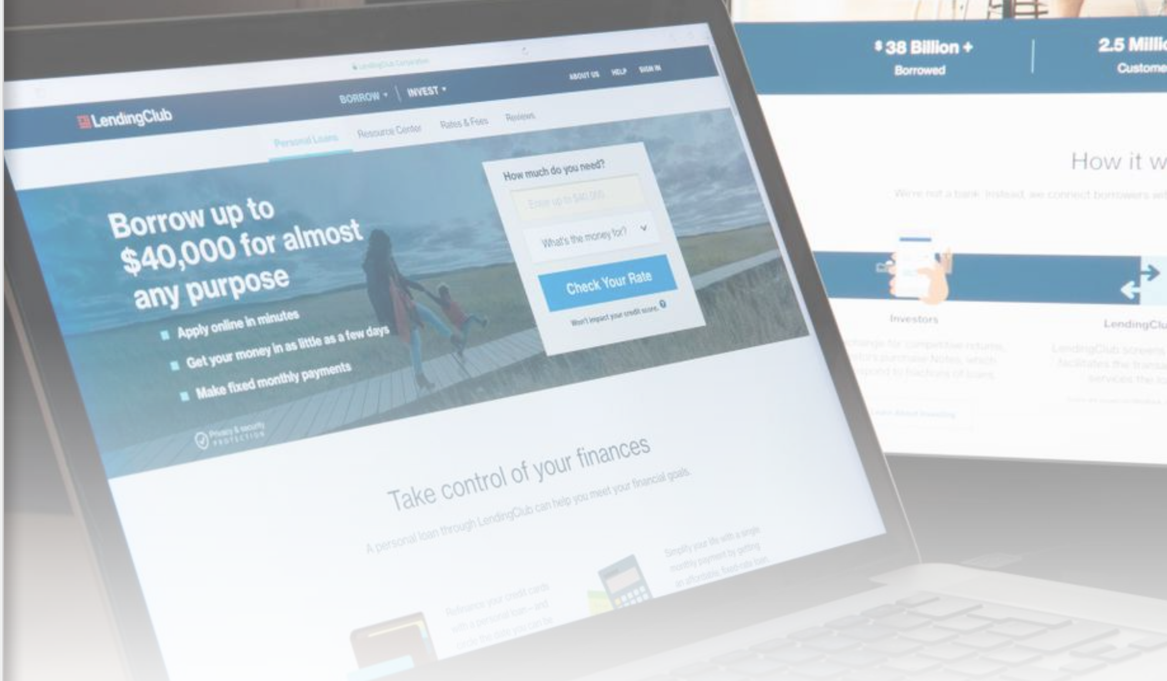
"Fraud incidents, both online and offline, have increased by more than 130% during the past year, resulting in significant monetary and reputational losses for financial institutions."

PwC

# Lending Club

Lending Club connects borrowers and investors with an innovative online marketplace that is  changing the face of finance. But just like every other financial services firm, Lending Club is responsible for protecting enormous amounts of critical financial and personal data. To augment their efforts, they needed a turnkey bug bounty program that could cut down their low signal-to-noise ratio and focus on fixing bugs as quickly as possible.

Lending Club chose HackerOne Bounty as their fully-managed bug bounty solution, giving them a seamless, end-to-end program. By leveraging HackerOne's expert triage analysis, Lending Club is able to take work off of their engineers and maintain faster response and resolution times. And the HackerOne platform gives their security team critical data so they can constantly improve their own program.



> The key benefits when partnering (with a bounty platform provider is) you get centralized reporting, you have a platform that you can integrate, and you have that source of truth.

**TY SBANO**

*Former Director of Security Engineering, Lending Club*

LendingClub

# Bounty Trends: Severity

About 60% of organizations on the HackerOne platform pay an average of $1,500 for critical vulnerabilities, which is a 50% ($500) increase from 2016. As organizations fix more vulnerabilities and harden their attack surfaces, bounty values naturally increase over time. This is due to vulnerabilities becoming more difficult to identify, thus requiring more skill and effort to discover.

The average bounty paid for critical vulnerabilities across all industries on the HackerOne platform rose to $2,041 in 2017. That's a 6% year over year increase from the 2016 average of $1,923.

Financial Services & Insurance, however, pays a comparatively low bounty for critical bugs. Their average reward of $1,118 is nearly double the previous year's average of $646, but is still comparatively low, ranking it third from the bottom across all industries.

Vulnerabilities by Severity

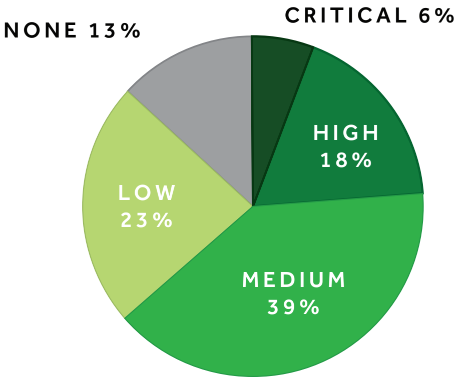


**Figure 4:** *The percentage of all vulnerabilities that are categorized as critical, high, medium or low severity. The "none" category represents vulnerabilities that did not register on the severity scale.*

Average Bounty Payout Per Industry for Critical Vulnerabilities

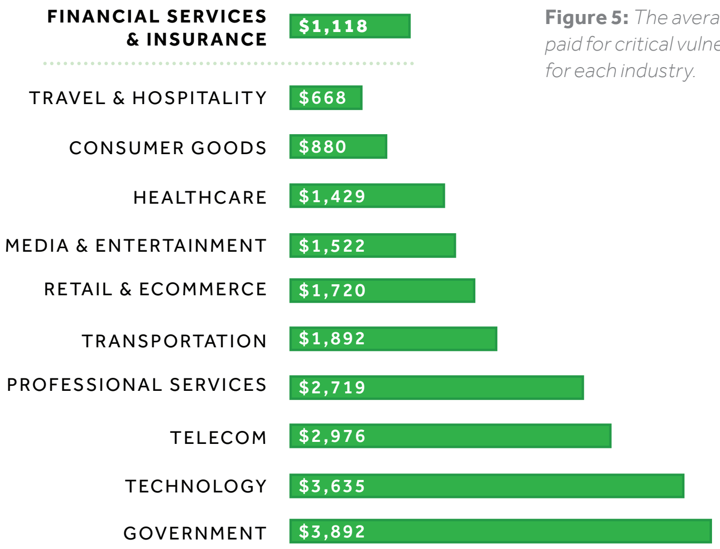


**Figure 5:** *The average bounty paid for critical vulnerabilities for each industry.*

CUSTOMER SPOTLIGHT

# Coinbase

Coinbase is the world's most popular marketplace for buying and selling bitcoin, ethereum, and litecoin. They're also a trailblazer in hacker-powered security, starting their bug bounty program in 2012 and moving to HackerOne's platform in early 2014. Over the past 5 years, Coinbase has paid out more than $175,000 to the hackers helping them secure their service.

As shown in this report, the Financial Services & Insurance industry tends to lag well behind the leaders in bounty awards and top bounty payouts. Not Coinbase. They recognize the value higher bounties have in attracting more, and more of the best, talent to their program. Their top bounty, which covers remote code execution bugs, is $50,000. That puts them in the top echelon of bounties across all industries.

"Coinbase loves bug bounties," said Philip Martin, Director of Security at Coinbase, in a recent blog post. "We think they fundamentally change the economics of vulnerability reporting. Instead of a researcher facing a choice between using a vulnerability themselves, selling a vulnerability to 3rd parties or giving a vulnerability away for free, bounties present a good, legal, risk-adjusted return for the time invested by a researcher."

coinbase
Buy Bitcoin, Ethereum, Litecoin, and other digital currencies
Coinbase - Buy Bitco
Secure Wa

> We take security incredibly serious at Coinbase. HackerOne is an essential part of our comprehensive security approach that amplifies our effectiveness by engaging and rewarding the highly skilled ethical security researcher community focused on detecting and reporting critical vulnerabilities protecting our community.

**PHILIP MARTIN**

*Director of Security , Coinbase*

# Bounty Trends: Top Awards

From HackerOne's inception in 2012 through June 2018, organizations have awarded hackers over $31 million. More than one-third of that, **$11.7 million, was awarded in the past year alone**, reflecting the striking growth trajectory of hacker-powered security.

Some of the most advanced organizations offer bounty awards in the six-figure range, with Intel and Microsoft offering up to $250,000, and Google and Apple offering up to $200,000, to name just a few. Bounties for critical severity vulnerabilities in the tens of thousands of dollars are not only common, it's becoming expected for mature bug bounty programs.

The highest bounty awarded in 2017 was $75,000, paid by a Technology company for three unique vulnerabilities that, when chained together, produced a remote code execution (RCE) that required no user interaction to exploit. The exploit chain could have allowed an attacker to steal credit card information, deploy mass ransomware campaigns, take over user accounts, attack employee accounts, and access infrastructure code. These are the types of critical issues that are found exclusively with hacker ingenuity.

The top award in Financial Services & Insurance was $18,000 this year, nearly double last year's top award of $9,500 and a significant increase aimed at attracting more hackers. Although that individual award may seem high, it still pales in comparison to Technology's top award of $75,000, and places the industry fifth behind Transportation, Telecom, and others.

Since HackerOne's inception, **Financial Services & Insurance has awarded nearly $1.4 million in total bounties**. The total bounty payout places the industry fourth overall, but is an increase of $883,374 in just the past year.

## Top Bounty Awarded by Industry

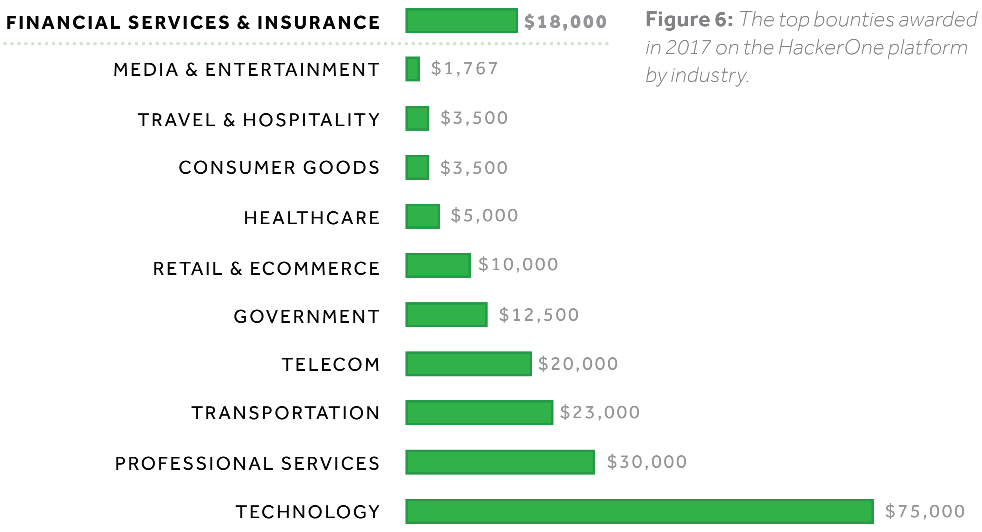


**Figure 6:** *The top bounties awarded in 2017 on the HackerOne platform by industry.*

## Total Bounties Paid by Industry

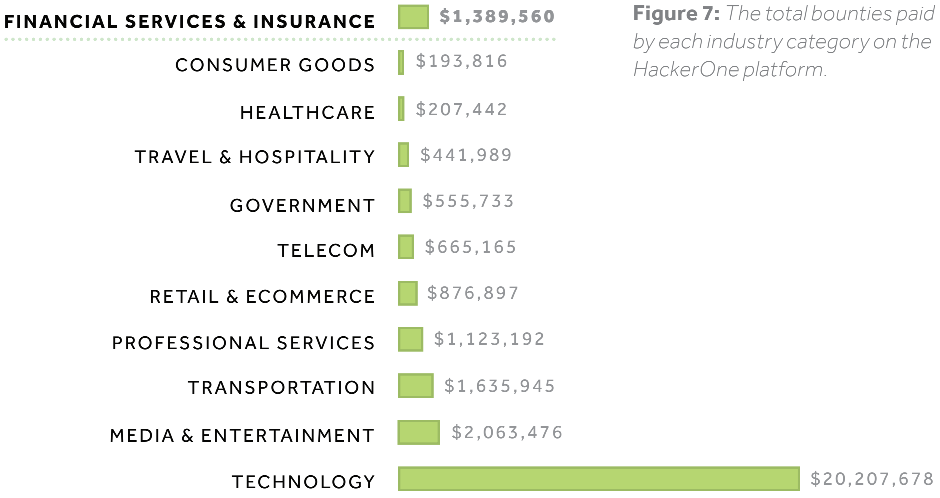


**Figure 7:** *The total bounties paid by each industry category on the HackerOne platform.*

## Working with Vetted, Trusted Hackers

Private programs give you complete control over which hackers are invited and who is eventually approved to participate in your program. HackerOne provides several layers of control for selecting, inviting, and validating hackers based on their Reputation scores, past program participation, specific skills, and more. Here's how it works.

**Step 1**. Identify and select hackers based on their activity on other bounty programs, as well as their Signal, Impact, and Reputation scores. Every hacker's activity and submission quality is tracked and incorporated into their Reputation.

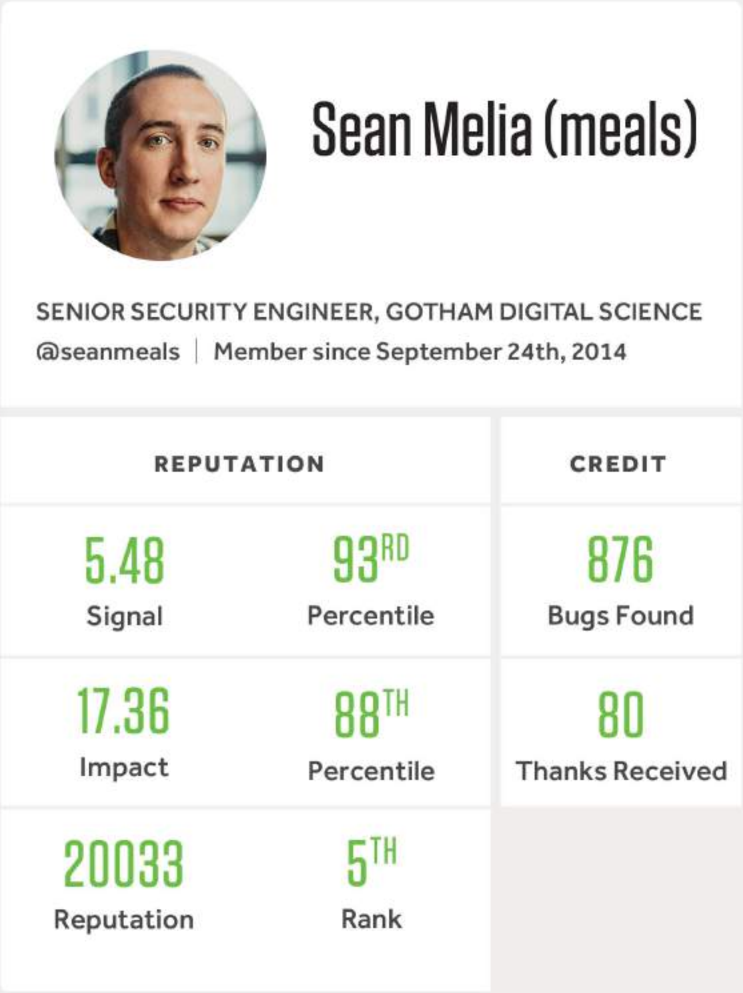
**Step 2.** Work with HackerOne to find the right hackers with the skills you need. Each hacker's profile page contains not only their Reputation scores, but also their "hacktivity", number of bugs found, thanks received, and badges earned. This offers a unique view into the skills and experience of each hacker, since hacktivity shows all previously resolved reports and, if public, the details of the actual report. Hackers can also add skills to their profile by submitting relevant reports that reference bugs in specific categories.

**Step 3.** Partner with your HackerOne Program Manager to determine if there are custom requirements you'd prefer, including NDAs, a robust application process, and even background checks.

Require even more control and hacker scrutiny? Then you need HackerOne Clear. HackerOne Clear allows you to work only with hackers who meet the strictest background and identity standards of the most demanding global organizations, such as the U.S. Department of Defense. Contact us to learn more.

SPOTLIGHT

### SAMPLE HACKER PROFILE

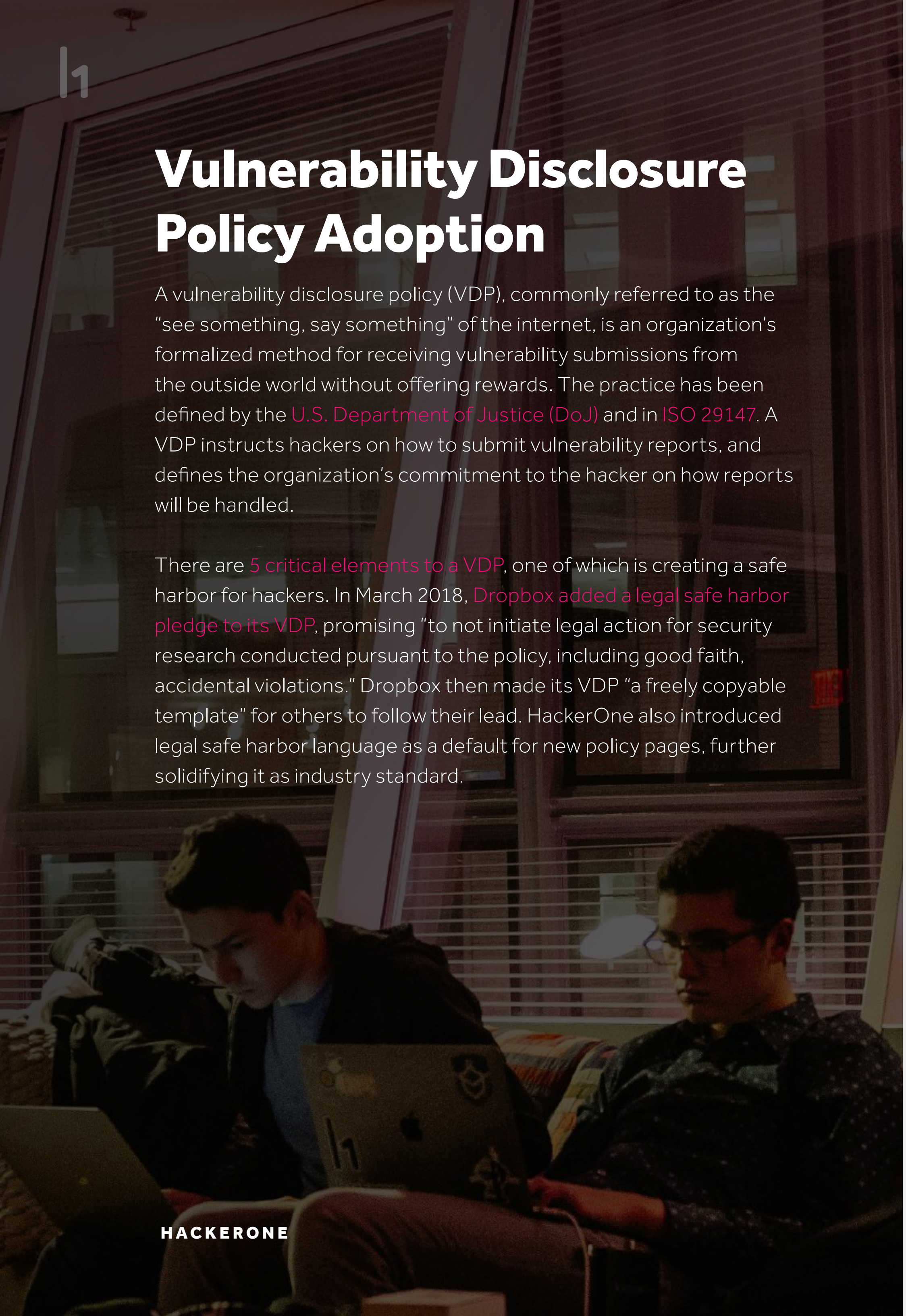


Sean Melia (meals)

SENIOR SECURITY ENGINEER, GOTHAM DIGITAL SCIENCE

@seanmeals | Member since September 24th, 2014

| REPUTATION | | CREDIT |
|---|---|---|
| 5.48<br>Signal | 93RD<br>Percentile | 876<br>Bugs Found |
| 17.36<br>Impact | 88TH<br>Percentile | 80<br>Thanks Received |
| 20033<br>Reputation | 5TH<br>Rank | |



# Vulnerability Disclosure Policy Adoption

A vulnerability disclosure policy (VDP), commonly referred to as the "see something, say something" of the internet, is an organization's formalized method for receiving vulnerability submissions from the outside world without offering rewards. The practice has been defined by the U.S. Department of Justice (DoJ) and in ISO 29147. A VDP instructs hackers on how to submit vulnerability reports, and defines the organization's commitment to the hacker on how reports will be handled.

There are 5 critical elements to a VDP, one of which is creating a safe harbor for hackers. In March 2018, Dropbox added a legal safe harbor pledge to its VDP, promising "to not initiate legal action for security research conducted pursuant to the policy, including good faith, accidental violations." Dropbox then made its VDP "a freely copyable template" for others to follow their lead. HackerOne also introduced legal safe harbor language as a default for new policy pages, further solidifying it as industry standard.

## Vulnerability Disclosure Policies: Guidance for Financial Services

In 2018, every industry is being implored to draft and publish a clear vulnerability disclosure policy (VDP) to partner with take advantage of the creativity and intelligence of the security community. VDPs are proven to reduce the risk of a security incident by finding and fixing critical security vulnerabilities before they fall into the wrong hands.

Financial Services & Insurance organizations are no different, and should be taking proactive advantage of the free and valuable input of the broader community of ethical hackers. In fact, leaders like Goldman Sachs and American Express have prioritized vulnerability disclosure policies, and you should, too.

To learn more, read "Vulnerability Disclosure Policy Basics for the Financial Services Industry".

# FORBES GLOBAL 2000: 93% STILL LACK VDPS

Each year, HackerOne analyzes the Forbes Global 2000 list of the world's most valuable public companies as one benchmark for public VDP adoption. Based on the 2017 list, **93% of the Forbes Global 2000 do not have a known vulnerability disclosure policy**. This is compared to 94% of the 2016 list not having VDPs. While these numbers have significant room for improvement, progress such as the VDP Framework recommended by the DoJ and Gartner's recent predictions that crowd-sourced security solutions will be employed by more than 50% of enterprises by 2022, up from less than 5% today, leave us hopeful.

The Financial Service & Insurance industry's coverage is nearly identical to that of the broader Global 2000, with approximately 93% of organizations in this industry lacking a public VDP. While leaders like American Express, Citigroup, JPMorgan Chase, ING, and TD Ameritrade have public VDPs, nearly every other Financial Service & Insurance organization on the list does not.

VDPs are designed to make it easy for any reported vulnerability to get into the right hands so it can be safely resolved. But until adoption of VDPs increases, vulnerabilities will continue to remain unreported. Nearly **1 in 4 hackers have not reported a vulnerability they found** because the company didn't have a channel to disclose it, according to our 2018 Hacker Report. Having a VDP in place reduces the risk of a security incident and places the organization in control of what would otherwise be a chaotic or nonexistent workflow.

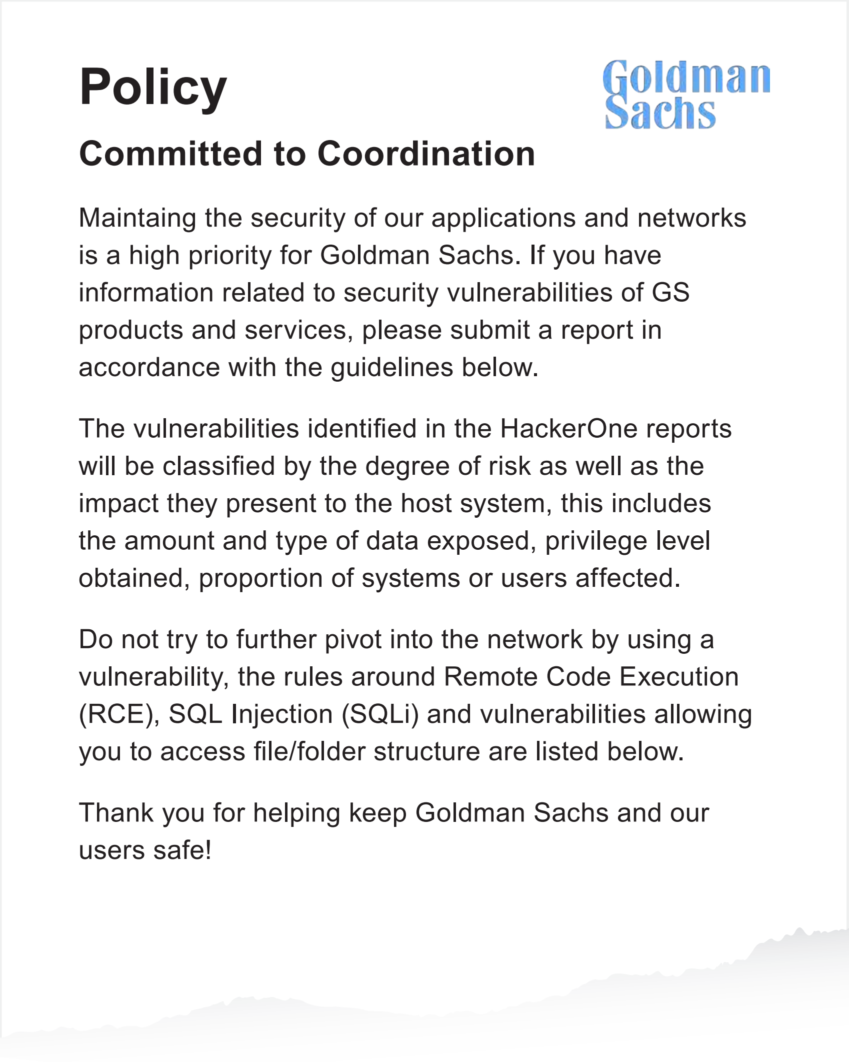
*How does the Financial Service & Insurance industry's public VDP coverage of 7% compare with other industries?*

- *47% of Technology companies have VDPs.*
- *24% of Telecommunications companies have VDPs.*
- *20% of conglomerates have VDPs or bug bounty programs, including General Electric, Siemens, Honeywell International, ABB, Philips and others—up from 14% in 2017.*

# Goldman Sachs

Goldman Sachs is one of the few Financial Service & Insurance organizations with a public VDP, which you can read in its entirety. Their security team is extremely fast at following up with discoverers, with an average response time of just 5 hours. And full resolution of bugs is typically completed in just 29 days.

In the first 3 months of their public VDP being listed on HackerOne, Goldman Sachs resolved 20 vulnerabilities and thanked 9 hackers.



## Policy

Goldman Sachs

### Committed to Coordination

Maintaing the security of our applications and networks is a high priority for Goldman Sachs. If you have information related to security vulnerabilities of GS products and services, please submit a report in accordance with the guidelines below.

The vulnerabilities identified in the HackerOne reports will be classified by the degree of risk as well as the impact they present to the host system, this includes the amount and type of data exposed, privilege level obtained, proportion of systems or users affected.

Do not try to further pivot into the network by using a vulnerability, the rules around Remote Code Execution (RCE), SQL Injection (SQLi) and vulnerabilities allowing you to access file/folder structure are listed below.

Thank you for helping keep Goldman Sachs and our users safe!

# Closing Thoughts

Hacker-powered security is a widely hailed method for improving security and reducing risk. As more organizations adopt it, and more government and industry agencies recommend it,  Financial Services & Insurance organizations will jump on board. When we all work together, cyber threats can be thwarted. Together we hit harder!

# Methodology and Sources

Findings in this report were collected from the HackerOne platform using HackerOne's proprietary data from over 1,000 collective bug bounty and vulnerability disclosure programs.

**Forbes Global 2000 Vulnerability Disclosure Research:** Our research team searched the internet for ways a friendly hacker could contact these 2,000 companies to disclose a vulnerability. The team looked for web pages detailing vulnerability disclosure programs as well as email addresses or any direction that would help a researcher disclose a bug. If they could not find a way for researchers to contact the company to disclose a potential security vulnerability, they were classified as one that does not have a known disclosure program.

Any companies that do have programs but are not listed as having one in the Disclosure Directory are encouraged to update their profile in the Disclosure Directory on their company's page. See ISO 29147 for additional guidance or contact us.

## ABOUT HACKERONE

HackerOne is the #1 hacker-powered security platform, helping organizations find and fix critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative. The U.S. Department of Defense, General Motors, Google, Twitter, GitHub, Nintendo, Lufthansa, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel, the CERT Coordination Center and over 1,000 other organizations have partnered with HackerOne to resolve over 78,000 vulnerabilities and award over $34M in bug bounties. HackerOne is headquartered in San Francisco with offices in London, New York, and the Netherlands.