Coda Payments Protects Their Brand with Better Visibility and Insights from RiskIQ

About Codashop and Coda Payments

Codashop, operated by Coda Payments, has become a trusted source of games and in-game currencies for millions of gamers worldwide. It enables users to choose from more than 250 safe and convenient payment methods and is visited more than 90 million times per month.

Coda Payments' mission is to offer the best value, experience and entertainment to its customers, every day, without fail. The vision is to be the platform of choice for taking life's digital experiences over the top by enabling users to bring more creativity and self-expression to their play—no matter who or where they are.

Founded in 2011, Coda Payments helps digital content providers monetize their products and services in more than forty markets. Publishers of leading games like Moonton (*Mobile Legends: Bang Bang*), Garena (*Free Fire*) and Tencent (*PUBG Mobile*), streaming platforms like *beIN* and *Bigo Live*, apps like *Tinder*, and video-on-demand platforms like *Viu* have integrated with Coda Payments to accept payments.

Coda Payments is headquartered in Singapore with dozens of additional outposts around the world. It is backed by Apis Partners and GMO Global Payment Fund, whose strategic management company is GMO Payment Gateway, Japan's largest online payment gateway. Coda Payments has recently been named the 28th fastest growing company in the Asia-Pacific region by the *Financial Times* (making it the second-fastest-growing fintech company in its region), the 8th fastest growing company in Singapore by the *Straits Times*, and a Technology Pioneer by the *World Economic Forum*.

Challenges

- Lack of visibility for internet-exposed assets
- Delayed identification of impersonating threat actors
- Needed remediation of threats to the Coda Payments brand

Solution Benefits

- Continuous discovery of Coda's owned assets
- Virtual users to engage with assets for better understanding of relationships
- Detection of brand infinging domains

Challenges

In addition to the public accolades, Coda Payments' success has generated unwanted attention from other circles. Today it is a target for malicious actors looking to capitalize on their brand visibility by mounting cyber campaigns using a variety of tactics including phishing attacks, fake social media profiles and rogue mobile apps. To proactively respond to these threats and protect its organization, customers and customer's end consumers, they required:

- Better visibility into what they owned that was exposed on the Internet
- Early identification of impersonating assets across all digital channels
- Enforcement actions initiated to remove impersonating assets on the Internet

The RiskIQ Solution

After evaluating the market, Coda Payments selected RiskIQ as their preferred cyber security partner and have implemented the following RiskIQ Solutions:

- **RiskIQ Digital Footprint®:** to provide continuous discovery of all of Coda Payments' owned assets visible on the Internet. RiskIQ virtual users regularly engage with these assets as real users would to understand the subcomponents, services and relationships of site elements and highlight anything requiring further investigation or remediation. This allows the security team to understand how Coda Payments is being viewed from the external world, from both a client and attacker perspective. This continuously updated footprint also provides a 'white list' of assets, reducing the time to identify and confirm impersonating or rogue assets.
- **RiskIQ External Threats®:** to provide brand security across the different digital channels including web pages, social media platforms, and app stores. RiskIQ detects the appearance of brand-infringing domains, brand infringing mobile apps in over 150 app stores, brand infringing social media accounts across the major social media platforms, and phishing sites leveraging Coda Payments' brands. Aligning with the internal workflow of Coda Payments' team, RiskIQ also provides a fully managed service to triage generated events and take down infringing assets.

The Results

The number of phishing complaints that Coda Payments receives has decreased significantly since the RiskIQ solution went live. Coda Payments' technical support and security personnel and RiskIQ's solution architects continue to refine operational practices to improve detection of and response to the external threats Coda Payments faces every day. From Feb to July 2021, there were a total of 69,295 detections of a variety of website phishing, fake social media profiles and rogue mobile apps out of which 52,360 had been resolved, through a combination of enforcement actions and internal review processes to ensure that the Internet assets of Coda Payments and their partners are not affected.

Conclusion

RiskIQ provides organisations with 'outside the firewall' visibility to discover unknowns in their digital attack surface and identify threats targeting their organisation and their customers. This actionable Intelligence can be used by security teams to address a wide range of security operations use cases to strengthen security and reduce overall cyber risk.

RISKIQ®

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com