Case Study

How ADR Protected a Health and Wellness Rewards Program with a Swift and Targeted Response

Introduction

Customer data security and transactional integrity are paramount in today's rapidly evolving digital reward landscape. Any security breach can lead to significant financial and reputational damage in the health and wellness industry, where incentives and rewards programs are vital for fostering participant engagement. This case study illustrates how All Digital Rewards (ADR) leveraged its robust Information Security policies and marketplace management tools to address an attempted fraud swiftly and effectively, ensuring the security of its client's rewards program while minimizing disruption to their business operations.

The Client's Challenge: Unauthorized Point Redemptions

Utilizing ADR's proprietary rewards platform, RewardSTACK™ a longstanding client in the health and wellness industry reported suspicious activity involving unauthorized point redemptions. Multiple customer accounts have been affected, with several redemptions happening outside the normal transactional patterns. The client immediately contacted their ADR Account Manager for assistance, as they were concerned about potential fraud within their program.

Given the severity of the situation, time was of the essence. The client needed immediate action to halt the fraudulent activity and prevent further damage while maintaining the integrity of the ongoing legitimate transactions.

ADR's Swift Response: Rigorous Security Protocols in Action

All Digital Rewards has always prioritized security, embedding rigorous Information Security policies and procedures across its operations. Within 20 minutes of receiving the client's alert, ADR's team initiated a series of critical steps to protect the client's rewards program from further unauthorized activity.

1. Immediate Marketplace Shutdown

ADR's first action was to disable all client marketplaces immediately. By swiftly taking these marketplaces offline, ADR halted any ongoing fraudulent redemptions, preventing further unauthorized transactions. This rapid response ensured that fraudulent actors could not exploit any more customer accounts, effectively carrying out the potential damage within minutes.

2. Controlled Reactivation of Unaffected Marketplaces

With the programs offline, the client took the lead in identifying the problem, as it originated on their end. Together, we worked closely with their team, analyzing transaction data to pinpoint the compromised accounts. Once the affected areas were identified, we carefully reactivated the unaffected marketplaces, ensuring legitimate users could continue accessing their rewards seamlessly.

This level of precision—deactivating only the compromised marketplaces and accounts—enabled the client to maintain business continuity. Customers who were not impacted by the fraud could still access and redeem rewards, minimizing disruption to the overall program, while ADR focused its attention on the fraudulent accounts.

3. Collaborative Investigation and Data Analysis

To thoroughly understand the extent of the breach, ADR partnered with the client's internal fraud and security team. They gathered essential data, including redemption patterns, user behavior, and accounting histories. Regular strategic meetings were held to ensure that both teams were aligned on the investigative process and that all necessary information was shared in real time.

ADR also recommended implementing new fraud prevention measures at the rewards program's front end. These included enhanced user authentication procedures, transaction monitoring systems, and additional security checks before redemption processes could be completed.

Key Actions Taken by ADR

- **Swift Marketplace Shutdown:** Within 20 minutes of receiving the fraud alert, ADR disabled all client customer marketplaces, halting unauthorized transactions and preventing further damage.
- **Controlled Reactivation:** ADR systematically re-enabled marketplaces that had not been compromised, ensuring business continuity for legitimate users and minimizing the overall business impact.
- **Collaborative Investigation:** ADR worked together with the client to gather the necessary data, investigate the root cause, and identify compromised accounts. They also advised on future preventive measures to enhance security.
- **Controlled Reactivation of Deactivations:** carefully reactivated the deactivated marketplaces, one at a time, as the client released them as GO LIVE, and those members affected saw their issues resolved quickly and efficiently.

Outcome: Minimizing Disruption, Maximizing Security

Thanks to ADR's swift and targeted response, the client could mitigate the potential damage caused by the fraud without experiencing a major disruption to their rewards program. The ability to selectively deactivate and reactivate marketplaces gave the client a level of control that few other providers in the reward platform space could offer.

The tailored shutdown process allowed unaffected markets to continue operating normally, maintaining high customer satisfaction despite the ongoing investigation. More importantly, the client was able to protect their customer data, preserve the integrity of their rewards system, and prevent future fraud by implementing ADR's recommended security enhancements.

Key Benefit: Operational Continuity with a Targeted Response

One of the standout features of ADR's platform, demonstrated in this case, is the ability to selectively disable and reactivate marketplaces. This functionality allowed the client to avoid a complete system-wide shutdown, which would have led to widespread customer dissatisfaction and significant business disruption.

Instead, by focusing on specific marketplaces and accounts, ADR minimized the overall impact of fraud while maintaining operational continuity for unaffected users. This level of control gave the

client peace of mind, knowing that their rewards program was protected without sacrificing the customer experience.

Furthermore, the quick response time and collaborative approach to resolving the issue underscored ADR's commitment to client security. The investigation also revealed valuable insights, which ADR and the client leveraged to further strengthen their program's fraud detection and prevention measures.

Why ADR's Security Measures Stand Out

This case exemplifies the strength of ADR's security protocols, reinforced by our HITRUST Certification and the flexibility of our marketplace management tools. Several key elements set ADR apart from other providers in the health and wellness rewards space:

- **HITRUST Certification:** ADR is proud to be HITRUST Certified, which ensures that our platform meets the highest standards for safeguarding sensitive information. HITRUST Certification is one of the most widely adopted security frameworks in the healthcare industry, and it demonstrates ADR's commitment to the stringent requirements for managing and protecting sensitive health and personal data. This level of compliance gives our clients in the health and wellness industry confidence that their customer data is handled according to industry-leading security practices.
- **Comprehensive Information Security Policies and Procedures:** ADR operates with a comprehensive suite of information security policies and procedures designed to protect client data and systems. These include robust data encryption methods, regular vulnerability assessments, multi-factor authentication for platform access, and strict access controls to limit exposure to sensitive information. Our policies are continuously updated to comply with evolving industry regulations and standards, ensuring that client assets are always protected.
- **Advanced Data Controls:** ADR's platform incorporates advanced data controls to prevent unauthorized access and ensure data integrity. We use secure encryption protocols for data both in transit and at rest, and our logging and monitoring systems provide real-time tracking of all activities within the platform. These controls help detect and prevent fraudulent activities and provide our clients with the transparency and oversight needed to manage their rewards programs confidently.
- **Rapid Response:** The ability to react to fraud in real-time is critical in minimizing damage. ADR's team was able to disable the client's marketplaces within 20 minutes of the fraud alert, a response time that is difficult for many other providers to match. Bring the unaffected marketplaces up and restore the client deactivated marketplaces as directed in a timely manner.
- **Tailored Approach:** Instead of resorting to a full shutdown of all systems, ADR's platform allowed for a more granular approach. By selectively disabling and reactivating specific marketplaces, ADR ensured the business could continue functioning with minimal disruption.

- **Collaborative Support:** Throughout the client's investigation, ADR worked hand-in-hand with the client, offering data support, strategic guidance, and recommendations for long-term security improvements.
- **Proactive Fraud Prevention:** Beyond addressing the immediate threat, ADR provided actionable insights to the client on bolstering their fraud detection systems. This proactive approach resolved the current issue and helped to future-proof the client's program against potential threats.

Conclusion: A Commitment to Security and Client Success

At All Digital Rewards, security is not just a checkbox—it's a cornerstone of our service. This case study shows the effectiveness of ADR's security protocols, our ability to respond rapidly to potential fraud, and the flexibility of our marketplace management tools.

In the highly competitive health and wellness industry, where rewards programs play a critical role in engagement, behavioral outcomes, and retention, having the assurance of robust security measures is essential. ADR's commitment to protecting client assets, ensuring minimal disruption to operations, and providing ongoing fraud prevention support sets us apart as a trusted partner in the Health and Wellness space.

For clients looking to maintain the security and continuity of their rewards programs, ADR offers a powerful combination of technology and expertise that delivers peace of mind. Whether it's responding to fraud or implementing preventive measures, ADR is dedicated to safeguarding the integrity of your programs while ensuring a seamless experience for your customers.

Don't wait until it's too late—ensure your rewards program is secure and resilient. Contact us today for a consultation and learn how ADR can provide the tailored secure reward management solutions you can trust.