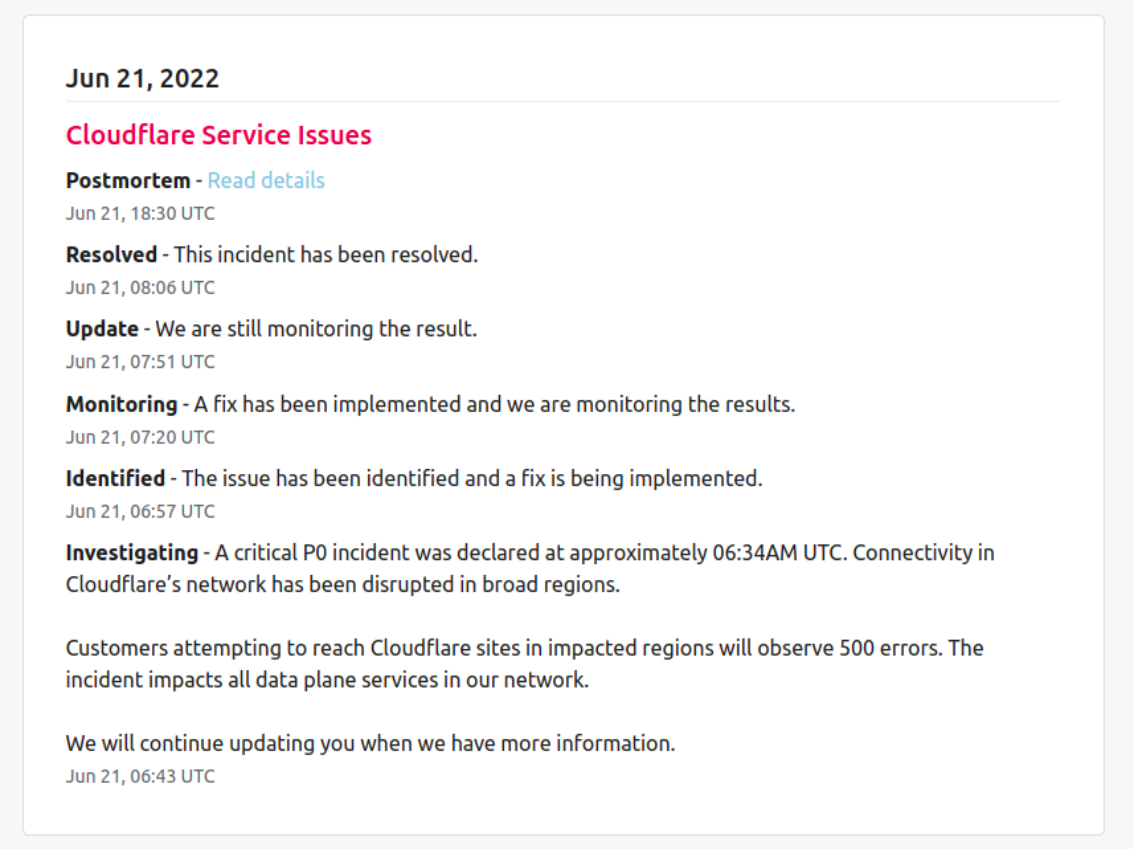
Incident Reporting Form - Revised RCA

1. Letter/ Report Subject -	Reporting of technical glitch to the exchange
Name of the Member-- **Member Code -**	Zerodha Broking Limited NSE: 13906, BSE: 6498
2. Designated Officer (Reporting Officer details)	
Name: Venu Madhav	
3. Date & Time of Incident & Incident duration	21-06-2022, 12:04 PM, 46 minutes
4. Incident Description & chronology of events **(please use additional sheets)**	Annexure 1
5. Business Impact	Annexure 2
6. Immediate action taken (please give full details)(please use additional sheets if necessary)	Annexure 3
7. Date & Time of Recovery	21-06-2022, 12:50 PM
8. Root Cause Summary **(Pl attach the detailed Report separately)**	Annexure 4
9. Back up measures available	Annexure 5
10. Details of long-term action (please give full details) **(please use additional sheets if necessary)**	Annexure 6

Annexure 1:

1. Connectivity to our trading platforms (along with many other websites across the globe) was impacted intermittently from 12.04 PM to 12.50 PM on 21-06-2022 owing to what seems to be intermittent connectivity issues via the Cloudflare network for users on certain ISPs.
2. Cloudflare is the vendor which provides content delivery network (CDN), network capacity, and DDoS protection to Zerodha.
3. We have attached the RCA obtained from Cloudflare which confirms that their service was impacted.
4. We have also attached the screenshot showing the status posted by Cloudflare about the outage which confirms that they observed Internet connectivity issues. (Sent as a part of the Intimation mail also).
5. Cloudflare identified the issue and deployed a fix that resolved the issue.
6. Cloudflare has published a postmortem report about the issue explaining in detail as to what went wrong.
7. 

Annexure 2:

There was an intermittent issue with the display of Orders, holdings & positions temporarily on Kite for some of our users.

a. The issue was Intermittent.
b. For those users who were impacted Call and trade desk was open.
c. The customers were informed to use alternative ISP or use the call and trade route.
d. The users were able to reach our website post multiple retries even when the issue was ongoing.

1. Number of Clients who were affected due to the Technical Glitch?

   Around 68000 to 80000 clients were intermittently impacted by this Technical Glitch.

2. The number of client complaints received with claims of losses due to the glitch on June 21?

   There have been limited customer complaints for this issue (about 180+ tickets and about 1800+ calls). However, all the clients have been convinced and there haven't been any refunds processed for claims of losses for this issue.

3. Were any alternate channels available to the clients? If yes, Was there any spike in traffic on the alternate channel during the Technical Glitch Incident?

   The issue was intermittent for different ISPs. Hence, the customers were informed to use an alternative ISP. When the users tried connecting via different ISP they were able to connect. The users were able to reach our website post multiple retries even with the same ISP as well.

4. Was the impact regional? If yes, what regions were affected due to the Technical Glitch Incident?

   No, the incident wasn't specific to a particular region.

Annexure 3:

1. A bulletin was put up on our website
2. A tweet was put out informing our customers about the incident.
3. A FCM push was also sent alerting the customers about the incident.
4. We raised an issue with Cloudflare immediately.

5. A lot of websites across the globe including a few stock brokers in India were impacted by this incident. Links to a few articles -
    a. https://www.moneycontrol.com/news/trends/even-downdetector-is-down-users-vent-after-cloudflare-outage-knocks-popular-websites-offline-8716691.html
    b. https://www.deccanherald.com/business/technology/zerodha-upstox-canva-down-as-cloudflare-suffers-another-outage-1120010.html

Annexure 4:

The final RCA (attached) received from Cloudflare confirms that:

1. The internet connectivity to our trading platform was impacted as a result of a problem at Cloudflare's end.

Our primary site was operational. This happened outside of our infra at the network capacity provider's BGP configuration. The network provider (Cloudflare) has many number of automated DRs and redundancies built in, where issues in any area of the network seamlessly migrate to other areas instantly. However, this issue was at the BGP level, affecting all the DRs across all networks across countries. This impacted a lot of websites across the globe including a few stock brokers in India were impacted by this incident. Links to a few articles -

a. https://www.moneycontrol.com/news/trends/even-downdetector-is-down-users-vent-after-cloudflare-outage-knocks-popular-websites-offline-8716691.html
b. https://www.deccanherald.com/business/technology/zerodha-upstox-canva-down-as-cloudflare-suffers-another-outage-1120010.html

Annexure 5:

Cloudflare is the vendor which provides content delivery network (CDN), network capacity, and DDoS protection to Zerodha. The main purpose for which we are dependent on Cloudflare is for Web Application Firewall (WAF). Cloudflare is our DNS provider and they resolve each request to their server IPs, analyze each request and only pass on safe requests to our actual IPs.

Cloudflare is already a multi-ISP, multi-network system, a network of networks. It was an extremely rare BGP incident that caused this. Cloudflare in itself is the redundancy and having another network of networks is extremely complex and infeasible.

Cloudflare is a network of networks, so there are many automatic redundancies built in. However, in case of continuous, prolonged, and total disruption to its many networks, we have the option to manually disable routing of traffic via Cloudflare's network and receiving end-user traffic directly to our servers from end-user terminals. The disruption on 21-06-2022 was partial and intermittent and affected a non-majority percent of users, which is why this option did not have to be exercised.

Annexure 6:

We recently obtained our own ASN registration and an IPv4 block to develop more sophisticated network setups in the near future. An internal timeline of 5 to 6 months - March 31, 2022 has been fixed for setting up the IPv4 block that will lead to the development of a more sophisticated network setup.

Additionally, Cloudflare has identified several areas of improvement and they will continue to work on uncovering any other gaps that could cause a recurrence.

They will immediately work on the following things:

Process: While the Multi-Colo PoP(MCP) program was designed to improve availability, a procedural gap in how they updated these data centers ultimately caused a broader impact in MCP locations specifically. While they did use a stagger procedure for this change, the stagger policy did not include an MCP data center until the final step. Change procedures and automation need to include MCP-specific test and deploy procedures to ensure there are no unintended consequences.

Architecture: The incorrect router configuration prevented the proper routes from being announced, preventing traffic from flowing properly to their infrastructure. Ultimately the policy statement that caused the incorrect routing advertisement will be redesigned by Cloudflare to prevent an unintentional incorrect ordering.

Automation: There are several opportunities in their automation suite that would mitigate some or all of the impact seen from this event. Primarily, they will be concentrating on automation improvements that enforce an improved stagger policy for rollouts of network configuration and provide an automated "commit-confirm" rollback. The former enhancement would have significantly lessened the overall impact, and the latter would have greatly reduced the Time-to-Resolve during the incident.