CDSL/OPS/DP/POLCY/2025/149 **March 3, 2025**

ADVISORY FOR FRAUDSTERS EXPLOITING COMPROMISED WEBSITES FOR PUBLIC DECEPTION

This is to inform the Depository Participants that cybercriminals have increasingly targeted websites of Depository Participants to perpetrate fraud, deceiving the public and potentially causing harm to both Depository Participants and Investors. These malicious actors exploit vulnerabilities in these trusted websites to carry out illegal activities; from stealing sensitive personal data to spreading false information.

How the Fraudsters Operate

Fraudsters typically use compromised websites as platforms to distribute counterfeit materials, such as official documents. In some cases, they even impersonate governmental or educational bodies, sending out fraudulent communications that appear legitimate. This makes it difficult for users to distinguish between authentic and fake information, increasing the likelihood of public trust being misused.

1. **Data Theft**: Hackers infiltrate various platforms to harvest sensitive data from unsuspecting users. This can include personal details, login credentials, or even payment information.
2. **Fake Documentation**: Fraudsters generate counterfeit documents, such as diplomas or licenses, using the compromised sites to give their documents a sense of legitimacy. These fake credentials can be used for job applications, immigration, or other services, allowing criminals to exploit public systems for personal gain.
3. **False Communications**: By making use of unofficial communication channels, fraudsters send emails or text messages that mimic official correspondence. These messages may ask recipients to provide personal details or make payments, often under the guise of needing to verify accounts or pay fees.

The Impact on the Public

Victims may face identity theft, monetary loss, or reputational damage. Furthermore, the impersonation of trusted websites erodes trust in these institutions, making users more vulnerable to future scams.

Prevention and Protection

It is crucial for Depository Participants to take proactive steps to mitigate these risks:

- **Stay Vigilant**: Be cautious about unsolicited emails, texts, or phone calls, especially those that request personal information or payments. Always verify the legitimacy of such requests through official channels.
- **Educate the Public**: Awareness campaigns about the signs of fraud and how to spot counterfeit documents can help users avoid falling victim to these schemes.
- **Brand Protection:** Depository Participants are encouraged to engage with Dark Web & Brand Monitoring solutions for comprehensive surveillance of a brand's digital footprint.
- **Strengthen Website Security**: Depository Participants should regularly update their security protocols, patch any vulnerabilities, and implement more robust authentication methods to protect user data.
- **Report Suspicious Activity**: If Depository Participants suspect they have encountered fraud, they should report it immediately to relevant authorities.

By taking these steps, Depository Participants can help mitigate the risks posed by fraudsters exploiting their digital assets.

Queries regarding this communiqué may be addressed to: CDSL on dpinfosec@cdslindia.com and connect through our IVR Number 022-62343333.

For and on behalf of
Central Depository Services (India) Limited

sd/-

Akhil Wadhavkar
Vice President– Information Technology