FACE

A short guide to defend against fraudulent use of company details[1]

Context

There is persistent proliferation of fraudulent and illegal lending, often misusing the details of the regulated entities (REs) or established Digital Lending Apps/platforms (DLAs/LSPs). Such fraudsters impersonate legal players by misusing company name, brand name, app, logo, address, CXOs/Director's name, website, registration certifications, CIN number and other propriety information to garner customer trust. These fraudsters exploit digital channels such as websites, social media, digital ads, web searches, and communication (email, SMS, telegram, WhatsApp, etc.), tricking customers into taking loans from unauthorised apps.

Such incidents harm customers, undermine the market trust and create business and reputational risks to REs/DLAs whose name fraudsters have misused. It is, therefore, important that companies of the digital lending ecosystem (REs/LSPs) keep an eye on the misuse of their identity by unscrupulous elements and promptly report them to relevant agencies for action.

Guidance

We guide FACE members to take the following steps:

Preventive

1. For legal coverage, register the trademark for the name, brand, logo and other proprietary information to protect against misuse, imitation and impersonation.

2. Stay vigilant on the unauthorised use of company name/logo and information (details like DLA, website, address, social media accounts, emails, CXO/Directors) across multiple digital channels. Companies may subscribe to anti-phishing / anti-rouge app services to identify and remove phishing websites/rouge applications.

3. Guard the company registration certificate with RBI, MCA, and other government IDs against unlawful uses[2].

4. Ensure that company emails on the own website/DLA, MCA[3] and RBI List[4] are correct and promptly respond to communication from law enforcement agencies, app stores and FACE to confirm the integrity of the website/app and association with DLA/LSP/RE, etc.

5. Maintain the updated information on the company's partnerships with DLAs, LSPs, and REs on the website/apps and ensure the same on partners' websites/apps, as applicable.

[1] Released on 4th Mar 2024. We prepared this guide drawing from our members experience in dealing with such episodes.

[2] For example, availability of company CoR on the website make it vulnerable to theft and misuse.

[3] https://www.mca.gov.in/content/mca/global/en/home.html

[4] https://rbi.org.in/Scripts/BS_NBFCList.aspx

6. Effectively use the company's social media handles to inform customers and stakeholders and prominently display social media links and contact details on the company website to raise awareness and contractibility of the company.

7. Customer grievance redressal can be another powerful channel as victims of such frauds are likely to reach out to genuine companies once they understand the threats from fraudsters. The customer grievance redressal system should have a process to report such cases on priority to the relevant department to examine further and take appropriate action. They should support the victims in reporting fraud to law enforcement authorities, as under:
   - https://cybercrime.gov.in/Webform/Accept.aspx
   - https://sancharsaathi.gov.in/sfc/
   - Cybercrime Helpline Number: 1930

8. Implement awareness programs for customers leveraging company outreach (website/apps/social media/newspaper) to prevent them from falling prey to fraudulent loan apps. Members may leverage the content available with FACE at https://faceofindia.org/consumer-corner/

Corrective

9. Once a company identifies a misuse, examine the case for channels used, potential impact, and scale of customer harm.

10. After there is an understanding of the specific misuse, report the episode at all relevant places, as necessary and relevant, as below:

    - Mobile Apps: Report the abuse to the app stores hosted by the app.

    - For Google Play Store/APK Files: Report as per information available here: https://support.google.com/googleplay/answer/2853570?hl=en&co=GENIE.Platform%3DAndroid. Trademark infringement can be reported to Google using this form. FACE members may send email to teamface@faceofindia.org for support.

    - If an off-Play apks are impersonating / are fraudulent, report them using this form: https://developers.google.com/android/play-protect/pha-reporting

    - If you believe an app on Google Play violates Google Play's Developer Program Policies, report them by completing this form: Report a Policy Violation - Play Console Help (google.com)

    - Website: Report fake websites on Google Search as per instructions on this link[5].

    - Facebook: https://www.facebook.com/help/contact/278770247037228.

    - WhatsApp: https://www.whatsapp.com/contact/forms/1534459096974129?lang=en_US.

    - Instagram: https://help.instagram.com/contact/779201836048501.

[5] https://support.google.com/legal/answer/3110420?hl=en

- LinkedIn: https://www.linkedin.com/help/linkedin/answer/a1338436.

- X (formerly Twitter): https://help.twitter.com/en/forms

- Contact the Grievance Appellate Committee[6] at https://gac.gov.in for appeals against delay/lack of response from social media and other online intermediaries.

- Report to the cybercrime department at the nearest police station. Company may also report online at the National Cyber Crime Reporting Portal: https://cybercrime.gov.in/

- If the company suspects[7] misuse from a website, social media, or email, it may report it to the National Cyber Crime Reporting Portal[8].

- Company may report the suspected fraud communications with the intention of defrauding telecom service users for cyber-crime, financial frauds, non-bonafide purpose like impersonation or any other misuse through Call, SMS or WhatsApp at https://sancharsaathi.gov.in/sfc/

- The company may also consider sending a legal notice to the developer, service provider, or platform for misusing their name, logo, trademark, etc. The company may approach the Court to seek Perpetual Injunction against the unauthorised users.

- The company should prominently inform customers and the general public from its website/social media about specific fraud incidents. As a matter of practice, if the scale of brand abuse is significant and frequent, it is advised to issue a public notice via newspapers.

- If the company is an RE, it may consider informing the RBI (for example, Regional Office[9]/Sachet Portal[10]/Daksha[11]) based on the impact and customer harm of the case as appropriate.

- For any suggestion/clarification/support on this topic, email us at teamface@faceofindia.org.

[6] https://pib.gov.in/PressReleasePage.aspx?PRID=1894258

[7] I4C, MHA has created this facility quick reporting of attempts made to commit cybercrime using suspicious Website URLs, Whatsapp Numbers/ Telegram Handles, Phone Numbers, Email-IDs, SMS Headers/ Numbers and social media URLs etc. This will be used to build up a repository for analysis and monitoring of cybercrime.

[8] https://www.cybercrime.gov.in/Webform/cyber_suspect.aspx

[9] Where company is registered

[10] https://sachet.rbi.org.in/Entity/Index

[11] https://www.rbi.org.in/scripts/FS_PressRelease.aspx?prid=54503&fn=2