DIY FRAUDBUSTER GUIDE

GATHER INTEL

There are several providers for these tools. Below are recommendations that tend to have more complete information.

1. **Find the registrar of the scam site by searching the domain at lookup.icann.org/en.**
   - The search result may include an abuse contact email or phone number.
   - Otherwise, search the registrar's website for abuse notification process.

2. **Find the IP address of the scam site domain using "Website to IP Lookup" at NSLookup.io.**
   - The search result may include an abuse contact email or phone number.
   - Otherwise, search the registrar's website for abuse notification process.

3. **Ask borrowers how they found the fraudster site.**
   - Links to referring social media profiles
   - Links to social media forums and/or groups
   - If via internet search, what search engine and term(s)

BUILD YOUR FILE

1. **Keep track of affected borrowers**
   - Name and contact details
   - Amount they were each defrauded
   - How they found the fraud site
   - Where they have submitted complaints
   - If their complaints name you/your business

2. **Document the fraud site.**

   You may consider an all-in-one site archiving software like Stillio (stillio.com), Pagefreezer (pagefreezer.com), or TrueScreen (truescreen.com)
   - Site screenshots that include the domain
   - Video recordings of a screenshare as you navigate the fraud site

3. **Track where you've reported (see next section)**

REPORT, REPORT, REPORT

Your goal here is to make law enforcement aware of (and proactively protect yourself from possible recourse), stop referral traffic, and take down the fraudulent site.

1. **Government agencies and law enforcement**
   - Attorney General—Your state and fraudster's "business location": www.naag.org/find-my-ag/)
   - Federal Trade Commission: https://reportfraud.ftc.gov
   - US Cybersecurity and Infrastructure Security Agency: email phishing-report@us-cert.gov
   - Federal Bureau of Investigation Internet Crime Complaint Center: www.ic3.gov/Home/FileComplaint
2. **Report abuse to domain registrar and website hosting service.***
   - Abuse phone number, form, or email from ARIN search results
   - DMCA takedown notice
   - Additional international resources via the World Intellectual Property Organization (www.wipo.int/members/en)
3. **Report referring social media profiles.**
   - Links to referring social media profiles
   - Links to social media forums and/or groups
   - If via internet search, what search engine and term(s)
4. **Report for blocklisting in web browsers and email services:**
   - Google (used by Chrome, Firefox, Safari): safebrowsing.google.com/safebrowsing/report_phish/?hl=en
   - Microsoft (used by Edge and IE): www.microsoft.com/en-us/wdsi/support/report-unsafe-site-guest

**Each provider will have their own reporting methods. Common methods:*

ALERT OTHERS

1. **Create a quick-reference sheet based on this Guide but with specifics of what to report and where to go.**
   - Fraud site information
   - Specific pages where phishing occurs
   - Registrar, hosting, and social media reporting links
2. **Send your quick reference to affected parties.**
   - Anyone whose logo or name also appears on the cloned site
   - Defrauded borrowers
   - American Association of Private Lenders

We will pass your sheet on to borrowers who reach out to us directly.

ENGAGE EXPERT HELP

AAPL Members receive a 30% discount off all Allure Security services. We have engaged Allure Security for AAPL brand and limited member site monitoring. We do not receive compensation or any affiliate fee for members who enlist their services. Reach us at contact@aaplonline.com for more information and to get started today.

ALLURE SECURITY

Both members and non-members may sign up for a free trial at https://alluresecurity.com/aapl.

1. **Domain and Web Impersonation Monitoring**
   (We recommend this for most members.)
   - Similar domain detection
   - Web beacon deployment (advanced cloned site alert)
   - Blocklisting from web browsers, email services, etc.
   - Data decoy injections into phishing forms
   - Fraud site take down
2. **Social Media Impersonation and Monitoring (brand and/or company executives)**
   We recommend this for larger lenders or lenders who have previously experienced impersonation attacks.
   - Monitoring on Facebook, LinkedIn, Instagram, Twitter
   - Profile take down