RECAP

THE FOLLOWING ARE COMMON FORMS OF TECHNOLOGY-ENABLED ABUSIVE BEHAVIORS:

1. **THREATS:** To inflict harm (physical/emotional/legal/financial/reputational), harm family or friends, self-harm, follow, humiliate, destroy property, spread rumors, post intimate images and more.

2. **UNWANTED CONTACT:** Messages, friend/follow requests, comments or tags on social media; emails; text messages; phone calls; contact via messaging app (whatsapp, kik, etc.), etc.

3. **UNAUTHORIZED ACCOUNT ACCESS:** Gaining access to online accounts or apps (email, social media, shopping, banking, rideshare, entertainment, maps, etc.) to intimidate, make changes, steal/delete information or engage in behaviors on this list.

4. **UNAUTHORIZED DEVICE ACCESS:** Gaining access to devices (smartphone, tablet, computer, smartwatch, wifi, smart speakers, home security systems, etc.) to intimidate, make changes, steal/delete information or engage in behaviors on this list.

5. I**MPERSONATION:** Inflicting reputational harm by hijacking a client's actual accounts or creating false accounts in the client's name.

6. **MONITORING:** Outside Job: Keeping tabs on the client by collecting publicly available online information about them; following the online/social media activity of the client (or their friends/family); joining a client's online groups; etc. Inside Job: Using unauthorized access to the client's accounts/devices to spy on them.

7. **LOCATION TRACKING:** Accomplished through social media monitoring, “safe” apps (find my phone, family sharing; find my friends, etc.), malicious apps/spyware installed on a client's device, tracking devices, etc.

8. **PRIVACY VIOLATION(S):** Doxing (publishing identifying information -- name, address, whereabouts, contact information, etc. -- of the client online); sharing personal/private/intimate information online; image-based abuse, etc.

9. **INDIRECT ONLINE ATTACKS:** Social media posts about the client; making false online complaints (personal or professional); tricking 3rd parties (businesses, strangers, etc.) into contacting the client online or in-person (at their home or work); spreading rumors online; signing the client up for accounts/services; triggering repeated security alert emails and notifications by attempting to access a client's online accounts; etc.