Cybercrime File Preparation Checklist Before Contacting a Lawyer in Abu Dhabi

Use this checklist to organize initial information and documents. You do not need every item. Mark what is available and let the lawyer determine the final requirements after reviewing the matter.

1. Identifying the Case and its Current Stage

☐ I identified the incident: extortion, fraud, defamation, hacking, impersonation, or a privacy violation.

☐ I prepared a chronological summary and identified my capacity: affected person, accused person, or company representative.

☐ I identified the current stage: before a report, investigation, trial, appeal, or enforcement.

☐ I recorded the next summons, hearing, or deadline and any continuing harm.

2. Parties and Account Details

☐ I recorded known parties, contact numbers, account links, and available identifiers.

☐ I explained my connection to each party or account and distinguished known facts from unknown information.

☐ I prepared basic identification details and any power of attorney or company authorization for an appropriate submission channel.

☐ I distinguished a compromised account from an impersonation account and recorded supporting facts without assuming who acted.

3. Facts and Digital Evidence

☐ I preserved complete conversations, messages, emails, files, and available original links.

☐ I recorded each item's source, time, time zone, and how it was lawfully obtained.

☐ I kept originals separate from working copies without changing content or relying only on cropped screenshots.

☐ I collected lawfully available login alerts, password-change notices, and account recovery requests.

4. Amounts and Losses

☐ I prepared transfer receipts and transaction records, including amounts, currencies, dates, and references.

☐ I recorded available beneficiary, wallet, network, and transaction details without private keys.

☐ I included contracts, invoices, advertisements, and promises connected to the transaction.

☐ I recorded harm, expenses, bank complaint references, and bank or payment-provider responses.

5. Reports, Proceedings, and Deadlines

☐ I collected available report numbers, summonses, minutes, reports, submissions, and judgments.

☐ I recorded the authority, service dates, upcoming deadlines, and any urgent measure.

☐ I documented content-removal or account-recovery requests and the platform's responses.

☐ I identified foreign parties or evidence and any translation or authentication requirements to be assessed.

6. Preserving Evidence and Organizing the File

☐ I created an index showing each document's name, date, and the fact it supports.

☐ I separated provable facts from estimates and information received from other people.

☐ I did not share passwords or verification codes or access accounts or devices without authorization.

☐ I avoided publishing private material, editing files, or resetting a device containing evidence before considering preservation.

Summary Ready to Send

Type of incident | My capacity and current stage | Upcoming deadline or continuing harm | Three most important available documents | Required legal outcome

Notice: This checklist is an initial organizational tool, not legal advice or a final determination of procedure. Arrange how to submit sensitive evidence with the team first.

© capitallawfirm.ae. All rights reserved.