Sample Legal Incident Report for Assistant Testing
To: Legal Assistant
From: Sharath
Date: 26 October, 2023
Subject: URGENT: Cybercrime Financial Fraud - Client: Mrs. Anjali Sharma

1. CLIENT BACKGROUND

Name: Mrs. Anjali Sharma

Contact: +91-98123-45678 | anjali.sharma@email.com

Address: B-104, Green Valley Apartments, Gurugram, Haryana - 122018

Profession: Retired School Teacher

2. SUMMARY OF THE INCIDENT

Our client, Mrs. Sharma, is a victim of a sophisticated "vishing" (voice phishing) and "phishing" attack, leading to unauthorized access to her bank accounts and a total loss of approximately ₹18,75,000 (Eighteen Lakh Seventy-Five Thousand Rupees). The fraudsters, impersonating bank officials, deceived her into revealing her Net Banking credentials and One-Time Passwords (OTPs), subsequently siphoning funds through multiple transactions to various accounts, including a merchant payment gateway.

3. DETAILED NARRATIVE OF THE FRAUD (Per Client Interview)

20th October, 2023 (10:15 AM): Mrs. Sharma received a call from a number appearing as +91-XX-XXXX-BANK (spoofed to look like her bank's official number). The caller identified himself as a "Senior Manager from the Bank's Fraud Department."

The Pretext: The fraudster informed her that a suspicious transaction of ₹25,000 was attempted on her debit card and that they needed to "secure her account immediately." To gain trust, they instructed her to check a genuine SMS from the bank regarding a "card block" (which they had triggered themselves).

Credential Harvesting: Under the guise of "verifying her identity and reversing the fraudulent transaction," the fraudster persuaded her to share her Net Banking User ID and Password. They assured her this was a standard security protocol.

OTP Compromise: Subsequently, she started receiving multiple OTPs on her mobile. The fraudster, who was still on the call, convinced her that these were "verification codes" to block the transaction and that she must read them out loud. She complied.

Discovery of Fraud: After the call ended, Mrs. Sharma received multiple SMS alerts from her bank (HDFC Bank A/c XX123) for actual transactions:

₹5,00,000 - Fund transfer to an account in ICICI Bank.

₹7,25,000 - Fund transfer to an account in Axis Bank.

₹6,50,000 - Payment to a "Digital Wallet Solutions Pvt. Ltd." (a merchant transaction).

Immediate Actions: She immediately called the bank's official customer care number from the back of her debit card to block her account and then visited the local bank branch. The bank officials advised her to file a police complaint.

4. FINANCIAL LOSS & EVIDENCE

Total Amount Lost: ₹18,75,000

Source of Funds: This amount included her life savings and funds set aside for her daughter's education.

Evidence Collected by Client:

Screenshots of the call log from her phone showing the spoofed number.

SMS logs from her bank showing the OTPs and the transaction alerts.

A copy of the written complaint she submitted at the HDFC Bank branch.

Bank statement highlighting the fraudulent transactions.

5. POTENTIAL LEGAL REMEDIES & APPLICABLE LAWS

We are considering action against:

The Unknown Fraudssters

The Bank(s) for potential failure in securing her account and allowing suspicious, high-value transactions without adequate secondary verification.

Applicable Statutes:

Information Technology Act, 2000: Section 66C (Identity Theft), Section 66D (Cheating by personation by using computer resource), and Section 43 (Penalty for damage to computer, computer system, etc.).

Indian Penal Code, 1860: Section 420 (Cheating and dishonestly inducing delivery of property), Section 468 (Forgery for purpose of cheating), and Section 120B (Criminal conspiracy).

6. INITIAL LEGAL QUESTIONS & TASKS

Please perform the following tasks to assist with the immediate course of action:

Drafting & Procedural Guidance:

Draft a comprehensive First Information Report (FIR) to be filed at the Cyber Crime Police Station in Gurugram. Ensure it incorporates all relevant sections of the IT Act and IPC.

Draft a formal Legal Notice to be sent to the Branch Manager of HDFC Bank, demanding immediate freezing of the destination accounts, a detailed transaction log, and provisional credit of the lost amount as per RBI guidelines on customer protection against fraudulent transactions.

Legal Research & Strategy:

Summarize the key provisions of the RBI Circular on 'Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions' (dated July 6, 2017). What is the bank's liability and timeline for resolution in a case like this, where the customer shared credentials but was duped?

What is the procedure for the police to issue a freeze order under Section 91 of the Cr.P.C. to the beneficiary banks (ICICI, Axis) and the merchant gateway (Digital Wallet Solutions)?

Investigation Support:

Prepare a list of specific pieces of digital evidence we should request from the client's mobile service provider and her bank to strengthen the case.

Identify the appropriate cybercrime agency (local police vs. a dedicated wing) in Gurugram for filing the complaint.

This is a time-sensitive matter. Please provide the drafts and your initial analysis by tomorrow, 27th October, EOD.