

Section: 66D Punishment for cheating by personation by using computer resource

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Under this provision case of online cheating can be registered. These may include the following



Nigerian Fraud / Lottery Scam / Advance Fee Scam: These scams are called Nigerian Frauds because in most of the cases nationals of Nigeria will involve. They are also called advance fee scams because in most of these offences a demand for advance fees will be there.

In these cases the course of offence will be gullible victims will receive unsolicited messages to the their mobile phones or e-mails are received to their email IDs mentioning their mobile numbers or e-mail ID have won million of dollars or pounds in Microsoft, International Cricket Cup draw etc, and victim are asked to contact to their e-mail IDs. If gullible people fall prey to these temptations, and then gradually amounts are asked to pay into bank accounts furnished by the fraudsters on different pretexts like advance fee, processing fee, transfer charges, fee to get no objection certificates (NOC), to get money laundering clearance, Income Tax Dept, etc. The fraudsters pretend that they are ambassadors, diplomats. There are instances where in the fraudsters come to the houses of the victims and hand over a suite case / trolley bags that contain a metallic chest. The incoming fraudster will open the chest and take out bundles of black papers and state that due to security reasons the prize amount is turned black and parcelled, and if the same is cleaned with a special chemical the notes will come to original form. To buy the chemical again amounts are

demanded. Ultimately the promised prize will never be paid because it does not exist at all.

On such complaints cases can be registered under the section 66-D IT Act because it is basically cheating by personation through e-mails and other electronic resource taking the names of different reputed organisations, and also pretending as ambassadors, diplomats. There is also deception, wrongful loss to the victim and wrongful gain to the fraudster hence section 420 IPC is attracted. The false e-mails (electronic records) with fake certificates in the names reputed organisation like Microsoft,, Yahoo etc are sent as if they are genuine; hence 471 IPC can also be invoked.



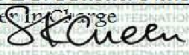


Form:
A36542

UNITED NATIONS ANTI-TERRORIST DEPT.
IN COLLABORATION WITH FEDERAL MINISTRY OF JUSTICE
HAGUE-NETHERLANDS.
Anti Drug/Terrorist Clearance Form
TO BE COMPLETED IN BLOCK LETTERS

SURNAME: _____
 OTHER NAMES: _____
 NATIONALITY: _____
 SEX: _____
 OFFICIAL ADDRESS: _____ TEL: _____
 E-MAIL: _____
BANKING INFORMATION:
 BANK NAME: _____
 BANK ADDRESS: _____
 ACCOUNT NO. _____
 SWIFT CODE: _____
 ROUTING CODE: _____
 SIGNATURE: _____ DATE: _____

OFFICIAL REMARKS FOR OFFICE USE

| ACCOUNT NUMBER | PARTICULARS OF THE ACCOUNT |
|-----------------|----------------------------|
| REMARK | |
| AMOUNT APPROVED | AMOUNT REQUIRED |

Signed, Dr. Prasad Nath
 Office in Charge




Online frauds – standard operating procedure (SOP):-

During the course of investigation

- All the e-mail correspondence between the victim and fraudsters shall be collected towards documentary proof to establish deception, demand for money etc.

Further, whatever bogus certificates i.e., 'winning certificate' 'immigration clearance certificate' etc that were sent to the victims

as attachments in the e-mails that were sent to victim shall be collected as prints towards documentary proofs.

- All deposit slips corresponding to the deposits made by the victim into different bank accounts as demanded by the fraudsters shall also be collected.
- The account opening forms of all bank accounts into which the amounts were deposited by the victims and transaction statements of them having been deceived by the fraudsters shall also be collected towards further documentary proof.

This information i.e., address as given in the account opening form, mobile number given to receive phone alerts, address & ID proofs given at the time of opening of the accounts can also be used to work out leads to detect the case.

The transaction statement of the bank account of the victim can be collected and the ATM centres from which cash withdrawals are made can be identified basing the ATM centre ID. From such an ATM ID further the physical location of the ATM centre can be identified and by contacting the concerned bank nodal team CC camera footages of the culprits can be identified and thus efforts can be made to identify the culprits.

- An investigative effort can also be made to trace the e-mail ID with IP Addresses. For this the full headers of the emails sent by the fraudsters shall be verified and the source IP address may be identified and such IP Address may be traced.
- Further in these cases the victims are contacted from different mobile numbers and hence for all such mobile numbers customer

application forms (CAFs) along with address proofs and ID proofs shall also be collected.

- After getting these entire can the case be detected? The answer is may or may not, because the addresses that may be identified basing bank account forms or SIM application forms may be insufficient, incorrect or false. However, all these laborious process of investigation shall be completed. The real challenge how to locate the culprits? The suitable answer for this could be while the fraudster is in contact with the victim over mobile number, such numbers can be tracked basing on mobile tower locations which is however difficult to zero in but the only feasible solution to detect these type of cases.
- If the fraudsters are identified a verification may be made with them for the presence of mobile numbers (SIMs) from which the victims were contacted while perpetrating the offence. Further verification may be made for the presence of deceptive e-mails that were sent to victims in their laptops. Such incriminating materials i.e., mobile phone, laptops etc shall be recovered and they shall be forwarded to the FSL for analysis and recovery of electronic evidence.
- While search is made at the house of Nigerians it is advisable such searches are conducted with a search warrant. Further if Nigerians are arrested care shall be taken that arrest information is given to the Nigerian Embassy. Further if Nigerians or other foreigners are arrested then addition of Sections 12 of Foreigners Act is also necessary because their involvements in an offence amounts to violation of the conditions of travel documents i.e., visa, passport etc

Other online frauds:-

Frauds by chatting friends:

Other variants of offences that can be registered under this provision are frauds committed by chatting friends. The people who chat online with strangers usually fall prey to these frauds. The chatting friend will pretend as business man abroad, and he has plans to expand hi business in India. In that process on one day he put forth his idea by saying that he is coming to India and after a few days he will call as if he is detained at the immigration check because he is carrying a valuable gift to the victim and request to pay clearance fee which will be in some lakhs into the bank account that he furnishes to get immigration clearance. Gullible victims without thinking the consequences pay and get defrauded.



Frauds over matrimonial websites:

Similarly frauds committed over matrimonial websites. The victims who have profiles on different matrimonial websites are contacted from purportedly a prospective grooms and gradually the confidence and affection of the victim are gained and using such good will amounts are collected from the victims. In these cases also the basic sections of law

attracted are 66 – D IT Act, then 420 IPC and as per the contents of the complaint other sections can also be invoked. The evidences that shall be collected include the registration details and profiles of the victim and also the accused. This information may be gathered from the concerned people of matrimony website as per the section 65 – B Indian Evidence Act so that the evidentiary value of it may be higher as it is collected from a neutral source. The deposit slips corresponding to the cash deposits made shall be collected from the victim. Required bank transaction statement as per 65 – B Indian Evidence Act or Bankers Books Evidence Act may be collected.

Frauds over classified websites like www.olx.inm, www.quikr.com etc

Further the offences that are committed by misusing the www.olx.com, www.quikr.com etc will also come under this category. www.olx.com, www.quikr.com are websites that allow people to post advertisement for selling their used or new items for free. Some fraudsters misuse this service and sell stolen goods, collect money but do not deliver any goods. In some other occasions the culprits post false classified in the names of other whom they want to harass. Sometimes false advertisement posts offering jobs in reputed companies will be posted on these websites and gullible job seekers are defrauded in the pretext of providing job through back doors methods.

Thus different types of online frauds can be registered and investigated under this section 66– D IT Act, and of course invoking other relevant provisions of IPC.

In these cases apart from following the line of investigation given above for the online frauds some specific case dependent evidences may be collected. In the case of fraud committed by chatting friends the chat logs

may be collected before mediators or at least they shall be collected from victim after getting prints attested by the victim himself.

With regard to the frauds over matrimonial websites the registration information and IP Address track of profiles of the victim as well as of the culprits shall be collected from the concerned service provider under certificate given as per section 65 - B Indian Evidence Act. Similarly the details of the false advertisement posts and their corresponding IP Address track logs may be collected from the classified service provider under a certificate given as per section 65 - B Indian Evidence Act.
