Name - Manish Arora **Mis - 111803036** **Btech Comp Div1**

Case Study of Cyber Crime Cases in India

Mphasis BPO Fraud

Ex-employees of MphasiS BFL's Call Center in Pune are the defendants in this case. They were instructed to have a polite chat with Citiban's global clients who call for difficulties with their credit cards and bank accounts when they first joined the call centre. The highest level of security is used in India's call centres. Employees are examined every time they come in and exit to prevent them from copying down account numbers. As a result, in this case, the employees must have memorised the number and gone to the cyber café shortly after leaving the office to access Citibank clients' accounts.

The money was subsequently transferred into the accounts that had been formed in Pune. Customers later claimed that their money had been transferred to accounts in Pune, and the culprits were tracked down. SWIFT, or Society for Worldwide Interbank Financial Telecommunication, was the service they utilised to send the payments. Fraudulent email accounts were created at the same time as fake bank accounts in Pune. The original account holders never received the confirmations that would have been sent during the money transfer. The money was transferred to a dozen bank accounts in March 2005, with the assistance of two ICICI home loan agents whose job was to facilitate the illicit accounts. They were among the non-BPO staff as well.

This theft raised a number of issues, including the role of **"Data Protection." Unauthorized access to clients' electronic account spaces** was used to commit this crime. As a result, we may determine that this case fits under the category of "Cyber Crimes." The Information Technology Act of 2000 is wide enough to cover certain forms of crime that are not codified in the Act but are covered by other laws. Any violation committed with the use of electronic documents under the **Indian Penal Code, 1860,** can be charged at the same level as crimes committed with written papers.

Section 43(a) - Compensation for failure to protect data.

Punishment - Because of the nature of illegal access that is involved in committing transactions, the Court decided that **Section 43(a)** of the IT Act, 2000 applies in this case. The defendants were additionally charged under **Section 66** of the same Act, as well as Sections 420 (cheating), 465, 467, and 471 (forgery) of the same Act.

Bomb Hoax mail In 2009

A 15-year-old Bangalore youngster was arrested on Friday by the city crime branch's Cyber Crime Investigation Cell (CCIC) for reportedly sending a hoax e-mail to a private news station. He claimed to have hidden five bombs in Mumbai in the e-mail, and challenged police to uncover them before it was too late.

According to authorities, the news station got an e-mail about 1 p.m. on May 25 that read, "I have planted five bombs in Mumbai; you have two hours to find it." The police were promptly notified, and the Internet Protocol (IP) address was tracked to Vijay Nagar in Bangalore. According to officials, the account's internet service provider was BSNL.

During the interrogation, Singh allegedly stated that he had no intention of committing any crime and was only curious as to what would happen if he delivered a bogus threat to a news channel via e-mail. Despite this, investigators said they extensively examined his computer.

After that there was steady increase in such cases by adults as well as some minors. The main purpose was “just for fun”.

Section 66A - Punishment for sending offensive messages through communication service

Punishment - Imprisonment for a term which may extend to three years and with fine.