# CAN A WHITE-COLLAR CRIME BE COMMITTED VIRTUALLY? IF YES, THEN WHAT LAW DO WE HAVE TO TACKLE THE SAME?

Rahul Kumar, B.A.LL. B, Lloyd Law College

## INTRODUCTION

Before we discuss, “white collar crime” we have to first understand what is “crime”. The word “crime” was originally taken from a Latin term “Crimean” which means “to charge” The Greek expression “Krimos” is synonymous to a Sanskrit word “Karma” which means “Social order” Therefore, **in common parlance the word crime is applied to those acts that go against social order and are worthy of serious condemnation.** An exact definition of ‘crime’ is by no way an simple task. Normally speaking, almost most of the societies have certain norms, beliefs, customs and traditions which are implicitly accepted by its members as a conductive to their well being and healthy development. Infringement of these cherished norms and customs is condemned as anti-social behaviours. Thus, many writers have defined ‘crime’ as **an anti-social, immoral or sinful behaviour.** However according to legal definition, **crime is any form of conduct which is declared to be socially harmful in a state and as such forbidden by law pain of some punishment.** Therefore, Tappan has defined crime as “**an intentional act or omission in violation of criminal law committed without any defence or justification and penalised by the law as felony and misdemeanour”**[1] To commit the crime there should be **Mens rea and Actus reus**. Mens rea means **mental element** and Actus reus means **physical element.** According to Blackstone, **A crime is an act committed or omitted, in violation of public law either forbidding or commending it**[2]**.** He, however realized that at later stage this definition may prove to be misleading because it limits the scope of crime to violations of ‘public law’ which normally covers political offences such as offence against the state. Therefore, he modified his definition of crime and stated **“a crime is a violation of ‘the people rights and duties’ due to the whole community” Stephan** the editor of Blackstone’

[1] Tappan Paul W: Crime, Justice & Correction, P. 80

[2] William Blackstone: Commentaries, Vol IV, P5

s commentaries further modified the above definition and said, **"a crime is a violation of right, considered in reference to the evil tendency of such violations as regard the community at large." Stephan** further added that "**crime is act which is both forbidden by law and revolting to the moral sentiments of the society"**[3] Thus, for act to be crime it must be in violation of law and at the same time it must be opposed to the moral sentiments of the society. It is essentially a relative definition of behavior that is constantly undergoing changing.[4]

## WHITE COLLAR CRIME

The notion of "white collar crime" found its place in criminology for the earliest time in 1941 when Sutherland published his research paper on white collar criminality in the American Sociological Review.[5] He defined **white collar crime as a "crime committed by persons of respectability and high social status in course of their occupation".** A white-collar criminal belongs to upper socio-economical class example, **misrepresentation through fraudulent advertisement, Infringement of patents, copyrights and trade-marks etc.,** are frequently restored to by manufacturers, industrialists and other person of repute in course of their occupation with a view to earning huge profits. Other illustrations of white-collar criminality include **publication of fabricated balance sheet and profit and loss account of business, passing of goods, concealments of defects in the commodity for sale etc.** This crime related to the corporate sector, white collar crimes are defined as **non-violent crimes**, **generally committed by businessmen and government professionals**. In simple words, crimes committed by people who acquired important positions in a company are called white collar crimes.

Generally white-collar crime can be separated into the following areas:

1. Corporate fraud: manipulating financial data, corporate insider self-dealing (including insider trading), late trading, misrepresenting net asset valuations, and so on.

2. Money laundering: hiding or disguising proceeds to make them represent to be from legitimate resources. These crimes are typically in conjunction with other crimes such as:

[3] Stephen's, *General View of Criminal Law of England*, p. 3.

[4] Prof. N.V. Paranjape, *Criminology and Penology* (14th edn. 2010).

[5] American Sociological Review Vol. V No 1 (1941).

health care fraud, narcotics trafficking, human trafficking, etc.

3. Securities and Commodities Fraud: Ponzi schemes, pyramid schemes, investment fund, embezzlement, etc.

In 2018, According to research published by The Economic Times, India was ranked 78th out of 180 countries, an improvement of three places from 2017. India is a developing country, and white-collar crime, along with poverty, poor health, and other factors, are contributing to its underdevelopment. White-collar crime is on the rise in India and around the world, posing a threat to economic progress. These crimes necessitated quick government intervention, not only in the form of tough legislation, but also in guaranteeing their correct implementation.[6] Mens rea is not required to establish a white-collar crime, but actus reus must be present. White-collar crime has calamitous consequences. In terms of the company, employees, customers, society, and so forth. White collar crime costs businesses a lot of money. To make up for the loss, these businesses boost the price of their product, which reduces the number of customers that buy it. Bank fraud is one of the most common crimes worldwide, as well as in India. Bank fraud is a crime done with the goal of deceiving others and obtaining unfair advantages. Fraudulent businesses commit it by making false representations. . It also involves the manipulation of negotiable instruments such as cheque bouncing, securities, and bank deposits, among other things. Bank fraud has an impact on the general people as well as the government. Vijay Malaya, Nirav Modi PNB Scam, Harshad Mehta, and other bank fraud cases are all affecting the government as a whole. Cybercrime is now having a greater impact on several countries. Cybercrime poses a threat to both national security and personal financial well-being. However, these crimes are also perpetrated by low-paid employees, even if the mastermind behind the crime is a wealthy individual with a better social rank in his field.

## VIRTUALLY COMMITTED WHITE-COLLAR CRIME

Most of the crime committed on the internet are white collar crime as they do not involve any violence and they are financially motivated. Before internet comes to existence these crimes are only outside the computer purview but now, they are occurring at a wide pace by the source of internet and cyber world. Any crime committed on the internet is referred to as cybercrime.

[6] Ibid.

White collar, cybercrimes seems to be sinless as there is a absence of violence and they do not happen on the streets. The laws for these crimes have enlarged their dimensions and we are getting more stringent laws for these white collars, cybercrimes. Lots of white-collar crimes occur on the internet every day. Here are some examples;

**1. Computer Intrusion (Hacking)**:[7] Cybercrime is a type of white-collar crime that occurs in real time on the internet. Hacking is defined as gaining access to a computer or the internet without sufficient consent or authorisation. Hacking is the manipulation of a computer's information system's inner workings. Hackers target a user's personal information for financial gain and monetary advantage. Hacking can be used for a variety of reasons. For example, someone accessing his family's email account qualifies as a hacker. The "Salami Attacks," which primarily occur in the financial sector, are a type of hacking that falls under the category of white-collar crime. Because they make such minor changes, these attacks go unreported. The Ziegler case, in which ten cents was deducted from the bank's account, is an example of a Salami Attack. It was happening in every deposited sum. Another similar attack occurred in May 2017 when the Wanna cry ransomware encrypting data demanded a ransom in the form of bitcoins cryptocurrency from computer users running the Microsoft Windows operating system.

**2. Cyber Fraud:** When a person intercept/ hacks the other person’s computer for accessing personal information which mainly involves credit card information, social security numbers, and other bank account information. Modern Example-Individuals and organisations must raise their knowledge of emerging cybercrime concerns as the threat of cybercrime grows with each passing year. The following are four types of common cyber fraud that businesses should be aware of.

### A. Social Engineering Attacks

Cybercriminals can use social engineering assaults as a low-cost, high-impact tactic. Cybercriminals, like legal firms, want to optimise profit while reducing operating expenses.

[7] https://blog.ipleaders.in/white-collar-crime-cyber-crime/

Social engineering attacks are well-positioned to achieve these objectives, thanks to a wealth of "as-a-Service" illicit software available on the dark web.

Successful social engineering exploits people's emotions by exploiting their fight or flight response. People frequently make hasty judgements when overcome by emotions such as fear or empathy. Initially, the pandemic, hackers used these emotions to launch successful phishing attack's typical themes included.

**B. Layoffs**

People were desperate for knowledge, which led to increasing profits as they relaxed their digital barriers. Whether they're targeting those looking for vaccinations, a return to "normal" living, or just comfort, this threat will persist through 2021 and beyond. Social engineering attacks are made more profitable by fear and uncertainty. Threat actors will see the viability of these schemes decrease in terms of cost-benefit analysis once this information becomes more concrete and available.

In terms of enterprise IT security, the situation in early 2021 was similar to that in early 2020. For example, according to a recent FortiGuard Labs Global Threat Landscape Report, web-based phishing lures and scams ranked first among techniques, until sliding out of the Top Five in June 2020. In brief, fraudsters focused primarily on social engineering assaults during the early months of the pandemic.

**3.Theft of identity:** Cyber crime related to the theft of data or data related crime. It occurs when the identity of one appropriated by other. There are different types of Identity Theft namely page jacking, ip spoofing cross-site scripting, etc. In Ip spoofing an individual impersonates the computer of the victim for accessing the privileged protocols without authorization, it is done by the help of software.

**Example: -**

***PHISHING-** it uses fake email-ids or messages containing virus affected website. These infected website urge people to enter their personal information such as login information, account's information.

### Attacks including phishing

### The sender

In a phishing attempt, the sender impersonates (or "spoofs") a trustworthy person who the receiver is likely to recognise. It might be a family member of the recipient, the CEO of the company they work for, or even someone famous who is apparently giving something away, depending on the sort of phishing attempt. Phishing emails sometimes resemble communications from huge firms such as PayPal, Amazon, or Microsoft, as well as banks or government agencies.

### The message

The attacker will ask the victim to open a link, download an attachment, or give money under the pretext of someone they trust. When the victim opens the message, they are confronted with a terrifying message designed to override their better judgement by instilling fear in them. The message may instruct the victim to visit a website and take immediate action or face repercussions.

### The destination

Users who fall for the lure and click the link are taken to a spoof of a legitimate website. They'll be asked to log in with their login and password credentials from here. If they are duped into complying, the attacker receives the sign-on credentials and uses it to steal identities, steal bank accounts, and sell personal information on the black market.

### Why is phishing victorious?

Unlike other types of online threats, phishing does not necessitate a high level of technological knowledge. "Phishing is the simplest sort of cyberattack, yet at the same time, the most deadly and effective," says Adam Kujawa, Director of Malwarebytes Labs. That's because it goes after the world's most susceptible and powerful computer: the human mind."

Phishers use social engineering rather than trying to exploit a technical flaw in your device's operating system. No operating system, no matter how secure, is totally immune to phishing, from Windows and iPhones to Macs and Androids. In reality, when attackers are unable to identify any technological flaws, they frequently resort to phishing. Why waste time trying to break through multiple layers of security when you can deceive someone into giving you the key? The weakest link in a security system is almost always a human who doesn't double-check where an email came from, rather than a bug buried in computer code.

**Phishing attacks come in a variety of shapes and sizes.**

Despite their various variations, all phishing attempts have one thing in common: they exploit a false pretence to obtain goods. The following are some of the most important categories:

**Phishing via email**

One of the most popular types of phishing is email phishing. It has been around since the beginning of e-mail. The attacker sends you an email posing as someone you know and trust (online store, bank, social media company, etc.) and instructing you to click a link to do a critical action or download an attachment.

The following are some examples of email phishing:

Business email compromise (BEC): A business email compromise (BEC) attack seeks to trick someone in an organization's finance department, usually the CFO, into transmitting huge quantities of money. Social engineering is frequently used by attackers to persuade the target that sending the money is essential and vital.

Clone phishing: Criminals make a copy—or clone—of previously delivered but valid emails that contain either a link or an attachment in this attack. The phisher then replaces the URLs or attached files with malicious substitutes that look exactly like the original. Unsuspecting users either open the attachment or click the link, allowing their systems to be hijacked. The phisher can then use the victim's identification to impersonate a trusted sender to other victims inside the same company.

419/Nigerian scams: One of the Internet's earliest and longest-running scams is a lengthy phishing email from someone pretending to be a Nigerian prince. This "prince" either promises you money but requires you to send him a modest amount first to claim it, or he claims he is in financial problems and need dollars to address it. This fraud is linked to the number "419." It refers to the portion of the Nigerian Criminal Code that deals with fraud, as well as the charges and punishments that can be imposed on those who commit it.

Case-RBI PHISHING SCAM

In this, there was a scam where the user gets a notification that they can win ten lakh rupees in merely forty-eight hours and after clicking that they reached the site looking exactly similar to RBI site. The user gives the personal information like password, account number etc.

***E-mail/ SMS spoofing-** The spoofed e-mail is one which shows its origin to be different from where it actually originated. In SMS spoofing, the offender steals identity of another person in the form of phone number and sending the SMS via internet and the receiver the form of phone number and sending the SMS via internet and the receiver get the SMS from the mobile number of the victim.

Spoofing is the act of misrepresenting messages to make someone believe they are coming from a legitimate source, as the term suggests.

Email spoofing, caller ID spoofing, website spoofing, IP address spoofing, SMS spoofing, and DNS server spoofing are all examples of spoofing.

In email spoofing, the email address is frequently very similar to a valid email address, giving the impression that it is coming from a trusted source. However, there could be a mistake somewhere. Instead of "info@inspiredelearning.com," the sender's address might be info@inspiredelreaning.com.

A keen employee might discover that the domain name in the first address is incorrect.

Employees who are distracted and unwittingly make little errors, on the other hand, rarely check for them.

Spoofing either be a harmless prank or the start of a terrible data breach that costs businesses millions of dollars in lawsuits and loses customers' trust. This is why it's vital to train your personnel to be more attentive and implement other safeguards to prevent spoofed messages.

## What Is Spoofing and How Does It Work?

### Spoofing a website

All an attacker needs to do with website spoofing is construct a replica of the domain they're impersonating. They'll utilise genuine logos, fonts, layouts, and wording to make you believe the website is safe to enter your personal information on.

When it comes to website spoofing, the web address is important to watch out for because it often seems identical yet contains a misspelling.

### Spoofing SMS and Calls

Attackers employ third-party software to convert the phone number they're using into an alphanumeric format that looks like a real phone number in SMS and call spoofing.

This software was designed with police enforcement, government entities, and businesses in mind, so their numbers will be clearly identifiable. Fraudsters, on the other hand, have utilised them to deceive their victims.

Using a fictitious phone number, attackers will send SMS text messages or spam phone calls, frequently with "urgent" action items. They'll even utilise your area code to make it look more genuine.

### A. Email Spoofing Email spoofing is another typical tactic used by con artists to get what they desire.

Changing the "from" email address to something that seems real or extremely close to an email address/sender ID you might expect is one method of spoofing email messages. To change their sender address, the attacker could be utilising another email client or internet scripts.

There are three suggested email authentication protocols you should have in your system to avoid email spoofing: Sender Policy Framework (SPF), DKIM, and DMARC.

Spoofing attacks are commonly used in conjunction with phishing to persuade you to click a link, enter sensitive login information, credit card numbers, physically transfer money, or communicate with the attacker in any manner.

Because phishing attacks frequently include spoofing and impersonation, because phishing assaults sometimes incorporate spoofing and social engineering techniques, the terms spoofing and phishing are frequently interchanged, even though they are two distinct techniques. Business email compromise (BEC), spear phishing, and whale phishing are other tactics that combine these two.

### How to Protect Yourself from Phishing Messages

So, how do you safeguard yourself and your company against spoofing messages?

Here are a few pointers you may share with your staff to help them avoid an attack and improve their security: -

1. Do not click on links that prompt you to take immediate action that you did not initiate.

A verification email from a service or programme, for example, even if you haven't signed up, logged in, or interacted with them recently, is an example of this. These notifications make you feel as if something urgent needs to be done, increasing your likelihood of clicking the link.

If you detect any unusual activity in your inbox, be cautious because it could be a faked email.

The link could include malware or lead to a faked website that imitates a legitimate service login page. To be safe, avoid clicking on the link in the message and instead go directly to the platform. You can then check on your account or even contact us to a representative to report the spoofing behaviour and/or to ensure you are not obliged to take any action.

2. Avoid clicking links from unidentified or unprompted sources in general.

When you get a strange email, this is a solid rule of thumb to follow. If you believe the source is trustworthy, instead of clicking the link, type the address into your browser directly. Manually inputting the link may assist you in detecting any errors, which are a red flag for a scam. If you click on infected links in text messages, emails, or social media phishing, malware will enter your device, extracting crucial information and compromising any data.

3. Make an investment in anti-malware software and email encryption.

Despite the fact that most email service providers have a good spam filter, some spam emails will still get through. One highly persuasive email is all it takes to put yourself or your company at danger of a data breach.

Endpoint security systems that block and notify end-users of questionable messages are examples of cybersecurity products. Furthermore, anti-malware software will analyse your system for known risks, remove the infected item from your network, and safeguard it from intrusions.

4. Don't open attachments from someone you don't know.

Attachments, like links, are a way for malware to get into your system. Downloading attachments, particularly from unknown sources, puts your computer at risk. The attachment could potentially be disguised as another file type (for example, text.txt.exe, which will appear as a text file with the.txt extension if you use the default file manager setting), which isn't a good indicator because most devices hide the file type by default in their file manager.

5. Become acquainted with the types of emails/messages that are most likely scammers (emails promising exclusive offers, money, etc.)

You should get aware with what messages are likely scams in addition to relying on your preventive software, such as antivirus and endpoint security. Teach your employees to think critically if they get a strange email. They may be distracted while going through their inbox, which is exactly what fraudsters want.

When you receive suspicious emails, such as ones that are unprompted, out of character, or ask for money or information, or offers that seem too good to be true, be cautious. Learn typical scam language and approaches, and make sure your employees are aware of them as well. This will help them be more cautious.

6. Check for grammatical or spelling errors.

The most obvious red flag in identifying faked messages is a typo, especially in the sender address in the case of email spoofing or the URL address in the case of website spoofing.

Scammers rarely double-check the messages they deliver because these attacks are typically hurried. It's very likely that the message sent will come off as odd, out of character, or with several spelling errors. If you suspect the message is a fake, keep an eye out for these types of errors and confirm with the sender via another channel.

7. Look up the email or message's contents on Google.

Thankfully, these con artists aren't as inventive as they'd like to be. The format of many scamming efforts is similar or identical since they are reused or copied from a template. If you receive a questionable message, you can check the information on Google to verify if it is genuine or not.

It's very likely that this isn't the first time this type of communication has been in someone's inbox, and that other people have wondered if it's a hoax.

8. Educate yourself on how to avoid spoofing.

If you've already received a spoofing message, it's simple to remember what you should do. In practise, though, it is more difficult to detect a spoof.

As a result, comprehensive training is required to raise staff awareness. Consider simulated training to ensure that your personnel remain aware and to demonstrate the deception of faked mails.

***Carding-** The cyber criminals make unauthorized use of the ATM debit and credit to withdraw money from the bank account of the individuals.

### The Process of Carding

Carding usually begins with a hacker gaining access to a store's or website's credit card processing system and obtaining a list of recently used credit or debit cards. Hackers could take advantage of flaws in the software and equipment used to protect credit card accounts. They could also obtain credit card information by scanning magnetic strips and copying the coding.

Carding is a type of credit card fraud that involves charging prepaid cards with a stolen credit card.

Credit card information could also be compromised if a hacker gains access to the account holder's other personal information, such as bank accounts, and targets the information at its source. The hacker then sells the list of credit or debit card numbers to a carder, who uses the stolen data to buy a gift card.

Most credit card issuers safeguard consumers from fraudulent charges if a credit or debit card is reported stolen; nevertheless, by the time the cards are cancelled, the carder has frequently made a purchase. Gift cards are used to buy high-value items like cell phones, televisions, and laptops, which don't need to be registered and can be resold later. If the carder buys an Amazon gift card, they may use a third party to receive the goods and then ship them to other places. The carder's risk of injury is reduced as a result of this attracting people's attention The carder could also sell the items on websites that provide some anonymity.

Because credit cards are frequently cancelled soon after they are lost, checking the stolen card information to see if it still works is an important component of carding. This could entail making purchase requests through the internet.

## Cases on white-collar crime:

### VARUPAL SINGH V. STATE OF PUNJAB

In this case, the petitioner was employed in motor vehicle company. The accused formed false bills and entry and deleted crucial data from the computer. Bills for the work done were deleted from the computer mainframe.

### BSNL CASE

A similar case has occurred in 2009 by a Technician from Bangalore named N G Arun Kumar where he was accused of altering the data of BSNL Broadband network. He got rigorous imprisonment of 1 year with 5200 Rupees fine u/s 420 of IPC [Cheating] and 66 of IT Act [Hacking]

## ENRON

A once-successful corporation resorted to strategies to hide losses and fake profits in this well-known white collar crime case. ENRON SHARES WERE WORTH $90.75 AT ONE TIME, BUT FOLLOWING THE COMPANY'S BANKRUPTCY IN 2002, THEY WERE WORTH ONLY $0.67. Using off-balance-sheet special purpose entities (SPVs) to hide rising debt and "toxic assets" from both investors and creditors was one of the unlawful acts involved in the Enron case. Andrew Fastow, the company's chief financial officer (CFO), was deemed substantially responsible for coordinating these deceptive business practises.

## WorldCom

The WorldCom probe began after internal audits discovered "improper accounting of more than $3.8 billion in spending over five quarters," according to CBS News, making it one of the "BIGGEST ACCOUNTING SCANDALS IN US HISTORY." Because these accounting discrepancies did not follow GENERALLY ACCEPTED ACCOUNTING PRINCIPLES, senior vice president and controller David Myers resigned, and more than 17,000 WorldCom employees were laid off.

## HealthSouth

According to The New York Times, auditors discovered "HUNDREDS OF MILLIONS OF DOLLARS IN PREVIOUSLY UNREPORTED ACCOUNTING FRAUD AT HEALTHSOUTH" in 2004. "$2.5 billion in fraudulent accounting entries from 1996 to 2002," according to the same article, "$500 million in inaccurate accounting äó_ and other things involved with acquisitions from 1994 to 1999," and "$800 million to $1.6 billion in 'aggressive accounting' from 1992 to March 2003." The entire number of false entries now stands between $3.8 billion to $4.6 billion. Richard M. Scrushy, the company's founder, was charged with 84 counts of fraud, and at least five former CFOs pled guilty.

## Bernard Madoff

Bernard Madoff, who was convicted of defrauding investors for $65 billion in 2009, is perhaps the most well-known white-collar criminal. His wealth management division collected money from investors to pay out to previous investors, never investing any of it. According to Investopedia, Madoff, the former chairman of Nasdaq and the founder of a renowned Wall Street firm, was sentenced to 150 years in jail for operating "a sophisticated PONZI SCHEME, which promised enormous returns on investments."

### Wells Fargo & Company

Wells Fargo, a banking and financial services company, is one of the most recent examples of a white-collar crime case. "Wells Fargo (WFC) EMPLOYEES SECRETLY CREATED MILLIONS OF UNAUTHORIZED BANK AND CREDIT CARD ACCOUNTS äóî without their clients' knowledge äóî since 2011," CNN Money reports.

Employees were able to meet unrealistic sales targets and obtain bonuses by opening 1.5 million bogus deposit accounts and submitting 565,443 credit card applications. Customers were then incorrectly charged fees for accounts they were unaware of. Wells Fargo must pay $185 million in fines and $5 million in refunds to customers who were harmed. This is the largest fine the Consumer Financial Protection Bureau has imposed since its inception in 2011.

## PREVENTIVE LEGAL MEASURE OR LAW AGAINST VIRTUALLY COMMITTED WHITE COLLAR CRIME

The most prominent service providers like yahoo, google, Hotmail, Facebook, twitter etc. are based in united states. Therefore, request for information related to cyber crime takes between 20 to 80 days which is too long a time. For the purpose of speedy exchange of information in cyber crime related cases, India has asked U.S. for setting up an Indo-American Alert Watch and warn time sharing of information for apprehending the perpetrators of these crimes.

Indian parliament also passed **Information Technology Act, 2000** to tackle down the increasement of cybercrime. Few important sections to prevent cyber white-collar crime: -

**Sec 65 and 66** of the IT Act deals with the act of hacking, whereas **section 70** of the Act defines the punishment for the same. Hacking includes various activities as per the law like introducing malicious software, destroying information, downloading of copies, interference, unauthorized access to the information.

**Section, 71** of the IT Act deals with cyber fraud i.e., Penalty for misrepresentation.

In India, before the 2008 amendment data theft comes under Section 66 of IT Act. But after the amendment, there has been the introduction of new offences in sections 66A to 66D in the IT Act.

## CONCLUSION:

Yes, after discussing different types of cyber crime we can say that clearly white-collar crime can be committed virtually for examples: Data fraud, hacking, theft of identity, Online gambling etc. are example of virtually committed white collar crime.