**Computer Crime II**

**Tutorial 4A**

Josh was extremely upset that his best friend of ten years, roommate and course mate at university, had the audacity to run off with his new-found girlfriend. Despaired by his friend’s treatment of the situation, Josh took his best friend’s wallet from the study table and left the twin room they both shared. With the money from the wallet, Josh bought several rounds of drinks at the local pub. It was not long that he found himself slightly tipsy as he stumbled back to campus.

While rummaging through the stolen wallet, Josh found a scrap paper which contained the scribbling of Personal Identification Numbers of automated teller machine cards, email accounts passwords as well as other confidential information. Josh thought to himself: why not steal some money from the guy that stole my girlfriend?

On reaching the Union Overboard Bank’s, a financial institution registered in Singapore, ATM, as Josh was about to insert the stolen card into the machine when he observed a poster informing the consequence of theft by unauthorised usage of ATMs. He gave it some though and was dissuaded by the message.

Again, back in his dormitory room, Josh wandered: since stealing money is wrong, then why not destroy the offending person’s social standing by sowing words of distrust of that person? With the login information on hand, Josh used his notebook to log into his best friend’s personal account on social network, SmileNetwork. While in there, Josh observed that his best friend had perpetuated the secret relationship for quite some time, unknown to many who knew both of them. Josh was definitely upset and decided to post a message to tell everyone in the network of his misdeeds.

However, Josh was too upset to pen anything. He decided to change his best friend’s login information to SmileNetwork so that he would have full control of that account, and that he could re-enter to post his message later. He then fell asleep in a drunken state.

Not long into the night, Josh was awoken by loud bangs on the door. Apparently, the police had been informed of Josh’s theft of his best friend’s wallet. Besides the stolen money, the police found that Josh had committed other illegal acts.

What offence(s), under the Computer Misuse Act, did Josh commit? Your answer has to be presented in the following format for **each offence**:

(i) Identify the issue(s) involved.

(ii) State the Law/legal principles.

(iii) Apply the Law/legal principles to the case, cite an appropriate reference case and provide a conclusion, which encompass the possible punishment.

1. **Issue**

Was Josh liable under Section 3 of the CMA when he entered his best friend’s personal account on social network SmileNetwork without authority ?

1. **Law/Legal Practices**

Section 3 of CMA

Unauthorised Access to Computer Material

Elements:

* Knowingly
* Causes a computer to perform any function
* Securing access
* Without authority

1. **Application**

Under section 3 of the CMA, Josh Knowingly caused a computer to perform a function that provided his access to his best friend’s personal account on social network without authority.

An example of this can be seen in the case PP v Lim Siong Khee (2001) where Lim was convicted after trial on a charge of knowingly causing an email server to perform a function for the purpose of securing unauthorised access to Ms Chong’s email account.

**Conclusion**

Josh was liable under Section 3 of the CMA when he entered his best friend’s personal account on social network SmileNetwork without authority

**Punishment**

Therefore, Josh had committed an offense under Section 3 of the CMA and he was liable to receive a maximum punishment of

* Fine not exceeding $5000
* Jail term not exceeding 2 years
* Or to both

**Issue**

Was Josh liable under section 5 of the CMA when he changed the login password to his friend’s personal account on social network SmileNetwork without authority

**Law/Legal Practices**

Section 5 of SMA

Unauthorised Modification of Computer Material

Elements

* Does any act
* He knows
* Unauthorised modification
* Of the contents of any computer

**Application**

Under section 5 of the CMA, Josh knowingly performed an act of unauthorised modification of the login password to his friend’s personal account on social network SmileNetwork

An example of this cam be seen in the case PP v Lim ZhaoMing Edwin (1999) where Lim was convicted after a trial on a charge of knowingly performed an act of changing of MediaCity’s website without authority.

**Conclusion**

Josh was liable under Section 5 of the CMA when he changed the login password to his friend’s personal account on social network SmileNetwork without authority

**Punishment**

Therefore, Josh has committed an offence under Section 5 of the CMA and he was liable to receive a maximum punishment of:

* Fine not exceeding $10,000
* Jail term not exceeding 3 years
* Or to both

\*\*\*\*\*\*\*\*\*\*\* IF MR MAH ABETS JOSH TO BREAK SECTION 5 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Issue**

Was Josh liable under section 10 of the CMA when he changed the login password to his friend’s personal account on social network SmileNetwork without authority

**Law/Legal Practices**

Section 10 of CMA

xxx

**Application**

Under section 10 of the CMA, Josh knowingly performed an act of unauthorised modification of the login password to his friend’s personal account on social network SmileNetwork

As such Mr MAH is guilty under section 5

An example of this cam be seen in the case PP v Lim ZhaoMing Edwin (1999) where Lim was convicted after a trial on a charge of knowingly performed an act of changing of MediaCity’s website without authority.

**Conclusion**

Josh was liable under Section 10 of the CMA when he changed the login password to his friend’s personal account on social network SmileNetwork without authority

**Punishment**

Therefore, MR MAH has committed an offence under Section 10 of the CMA and he was liable to receive a maximum punishment of:

* Fine not exceeding $10,000
* Jail term not exceeding 3 years
* Or to both