|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Identification of potential risk | Evaluation and assessment of potential risk | Assign ownership for each potential risk | Creative preemptive responses | Continuously monitor risk |
| 1. Fraud - Electronic payment systems are prone to fraud. The payment is done usually after keying in a password and sometimes answering security questions. There is no way of verifying the true identity of the maker of the transaction. As long as the password and security questions are correct, the system assumes the right person. If this information falls into the possession of fraudsters, then they can defraud the money. | HIGH | Students and Parents | New technologies such as EMV and fingerprint recognition are also being used by PSPs to reduce fraud. Advanced EMV technology is used to validate that a payment card is genuine and facilitate the authorization of the transaction. When a payment is made in-store, the card is inserted into a compatible card reader, the EMV chip is read, and data is exchanged in a highly secure manner, using encryption. Consumers are becoming increasingly familiar with biometric identification, such as fingerprint recognition, which is often used to unlock phones. It is now being introduced to increase mobile payment security and prevent fraud. | Continuous monitoring is required so that we can act faster as soon as the risk occurs. |
| 1. Payment conflicts - Payment conflicts often arise because the payments are not done manually but by an automated system that can cause errors. This is especially common when payment is done on a regular basis to many recipients. If you do not check your pay slip at the end of every pay period, for instance, then you might end up with a conflict due to these technical glitches, or anomalies. | HIGH | Students and parents | It’s important to constantly check your pay slip after every pay period ends in order to ensure everything makes sense. | Continuous monitoring is required so that we can act faster as soon as the risk occurs. |
| 1. Identity theft - When processing payments, it’s crucial to secure a wireless connection to prevent an outside user from reading and downloading credit card data and using that data to steal the cardholder’s identity. | HIGH | Students and parents | Your payment processor should provide online card data security protection that minimizes the risks from a data breach. | Continuous monitoring is required so that we can act faster as soon as the risk occurs. |
|  |  |  |  |  |