Did you know that the first six digits on your card are called a bank identification number or BIN. It identifies which bank provided the card and can also be used to commit fraud.

A bin attack involves fraudsters using software on a website’s payment page. After selecting a BIN, the software generates the remaining numbers testing thousands of combinations within minutes until a valid card number is found.

Compromised card details are then used fraudulently. BIN attacks can have many negative results. Each card attempted generates an authorisation fee, so large volume bin attacks could have a significant financial impact for you. What’s more, your store may be suspended until security is in place which can impact your sales.

Your business may suffer reputational damage, as card holders wonder why you have charged their card. Of course, all unauthorised transactions will need to be returned to the card.

Thankfully, there are measures you can take to protect yourself from BIN attacks. Use the risk management tools that come with your online merchant facility. Install software designed to protect you against BIN attacks such as a Captcha tool. Add additional protection such as EMV3DS which helps protect you against fraud by having the transaction verified by the issuer.

If you experience a BIN attack there are steps you can take to minimize the impact. Consider temporary suspending your website, test that your security tools are working as they should be, call NAB Merchant Fraud or your payment gateway provider for help. For more information on how to protect your website please contact NAB Merchant Services.