How safe is your online shopping?
By Gordon Clarke and Emir Hrnjic

The Wirecard scandal has revealed that even major companies involved in online payments may be disastrously unreliable and may even enable illegal transactions such as money laundering, according to the Financial Times. In fact, Visa and MasterCard allegedly had their suspicions about Wirecard since 2015 after they realised that the company had high levels of stolen card purchases and reversed transactions.

The internal file from 2017 shows that Wirecard processed payments for a variety of controversial and potentially illegal businesses. It also indicates that Wirecard may not have as many customers as claimed.

In fact, sceptics are warning that there might be more Wirecard–type scandals ahead due to unscrupulous accounting practices and poor internal controls, as well as technical security failures.

ONLINE PAYMENTS

While online payment has been exponentially growing for decades, the global pandemic has given it an unexpected boost. According to 2019 e-Conomy Southeast Asia report, the six largest Southeast Asian markets recorded S$600 billion in online payments last year, while they were projected to exceed S$1 trillion by 2025. Moreover, in the last few years we have also witnessed rapid growth of instant payments using e-wallets and account–to–account transfers initiated on the mobile handset.

The COVID-19 pandemic has accelerated this trend. Online purchasing soared due to worldwide lockdowns whereby people remained confined to their homes for months. For example, Bain & Company now expects digital payments to account for 67 per cent of total transaction values in 2025 – 10 percentage points above their pre-pandemic prediction.

With online shopping regarded as a norm, we have become desensitised to allowing the storage of our payment details by merchants and processors, whose security is likely inferior to that of financial institutions. While our credit card details are deposited all over the web, companies we trust have failed to keep our data safe.

According to Statista, over 164 million sensitive records were exposed in 1,473 data breaches in the United States alone last year, while fraud cost the world economy over US$5 trillion overall, according to Crowe.

The question arises on how safe our online shopping experience is and how service providers can and should protect us.

FRAUD DETECTION

In the card payment business, fraud defences include on-line authentication, chip card security using the international EMV standard, the CVV figure on the back of the card, the "3-D secure" approach, as well as encrypted messages and databases at banks. On top of that, most card issuers and processors use machine learning to flag suspicious transactions.

For instance, in Singapore, where the limits on instant payments and contactless card payments are increasingly high, the main defence against fraud is the instant SMS warning to the cardholder when an unusual transaction occurs. However, this does not work as well for overseas issued cards which must rely on notoriously unreliable cross-border SMSes.

Card payment transactions are relatively well protected, but instant account–to–account payments have very few of these facilities. There is clearly a need for heightened vigilance on the part of service providers, merchants, as well as others who hold databases of customer credentials and accept digital payments.

In our view, three actions would certainly minimise fraud risk. All merchants, Payment Service Providers (PSPs) and payment system operators should use security monitoring systems (either run by themselves or by specialised security companies), hold only tokenised account data in their customer databases and in transmitted messages, as well as use machine learning algorithms to detect suspicious transactions especially at the PSP level. While the latter is a massive topic that deserves its own commentary (or several of them), we will focus on two other actions.

MONITORING SYSTEM AND TOKENISATION

The first step in securing data and systems is to control the technology perimeter of the organisation, for both processing services and PSPs. This includes setting up a monitoring system, often called a Security Operations Centre (SOC), which is often a physical box containing the necessary software. The SOC contains machine learning algorithms that learn the normal patterns of data and system behaviour in a company or network and instantly flag deviations from historical patterns.

The SOC also requires IT staff who should be well–trained to act appropriately upon the monitoring alerts.

The monitoring system should detect attempts by external agents to log in to the company's system, which are surprisingly frequent. Some intrusions result in the planting of malware which can sit quietly in a system for months, gradually learning how valid payment messages are authenticated while informing its controllers. Then, it suddenly strikes by sending massive payments abroad as in the well-known attack on Bangladesh Bank a few years ago.

The monitoring software, however, should spot the communications made by the malware, identify it using an extensive library of malware signatures, isolate the problem, and, finally, alert the IT team to remove it.

But all this is to no avail if someone on the inside is colluding with criminals or being coerced to manipulate the systems and substitute false destination accounts – also known as mule accounts

– when payments are being sent. According to US publication Digital-First Banking, up to one in five account openings at present could be fraudulent.

The best solution to this is tokenisation (not to be confused with the "tokenisation" in the crypto industry), where all databases and messages contain a token that looks like a real account number instead of the actual account numbers. Widely used in the cards industry, for example in the ApplePay and Google Pay schemes, the token also carries instructions ("domain controls") which allow transactions to be executed only under a very specific set of circumstances. These may include a specific day of the month, or only once, or only for bill payments, or countless other specifics. Using tokens makes mule account substitution frauds extremely hard, even from the inside.

In an ideal world, payment companies and merchants would make it so difficult for fraudsters that the benefits from a lucrative sting – which may take months of time and effort as well as lot of investment – would simply not be worth the risk of being caught.

However, we are far from that utopia, and the risks to customers and their service providers are real and large. The exponential growth of online purchasing and a further dramatic increase during the COVID-19 crisis are making the solution even more urgent.

Gordon Clarke is Managing Director of Monetics, a Singapore-based payments consulting firm. Emir Hrnjic is an adjunct assistant professor at National University of Singapore (NUS) Business School and a co-founder of Block'N'White Consulting. The opinions expressed are those of the writers and do not represent the views and opinions of NUS.