Premier Brains
Accounting + Auditing

UPDATE

TOP FRAUD RISKS FOR 2021 AND BEYOND

1. *Email hacks leading to diverting supplier payments to fraudsters*

With the improvement of technology and various tools in place especially online payments and confirmation of bank account details online, there have been a going trend of instances where emails are hacked and tracked, whereby the bank details get changed on invoices without anyone being aware of it. There can be instances where the fraudsters may even write emails using anonymous email accounts.

How businesses can protect against a risk like this? Below are some tips,

- **RECHECK BANK ACCOUNT DETAILS**

If making payment to a supplier for the first time, do not just simply rely on the invoice copy received over email, rather reconfirm the payment details over a call or verify through a more another authenticated medium. Other mediums could be fax, whats app, skype but should be completely off the emails database.

If it is an old supplier and bank details are already with you, be careful that if an email comes with different bank details, you must reconfirm the payment details over a call or verify through a more another authenticated medium

- **TRANSFER FUNDS IN ACCOUNT NAME OF SUPPLIER ONLY**

There can be instances where supplier invoice ask for funds to be paid to personal account of someone mentioned on the email. This is very risky, be very careful that funds are going for what you are paying for. Always choose to ask trade license of the supplier you are paying which is a valid one to ensure you pay exact as the name appears on the trade license.

- **DO NOT RELY ON EMAILS AS A BASIS TO CONFIRM CHANGING DETAILS**

If there are emails reconfirming the details or insisting on payments, do not rely on the same as there can be fraudsters writing that to you!

- **USE UPDATED ANTIVIRUS/IT PROTECTION SYSTEMS**

Employ best resources in protecting security of your database as it can expose the company to hacks without knowledge to the user and it can also indulge into personal database.

2. Phishing Evolving Dangerously

In one of the new worrying fraud trends: many companies and individuals are losing valuable assets without giving away passwords. This is a sign of an increase in the sophistication of phishing fraud techniques.

There is a growing trend of hacking into email accounts whereby criminals study the trend of emails been sent and use the right moment to amend supplier invoice whereby directing payments to be made to their bank accounts. Many times emails are not even written by the supplier but by the hacker. This has resulted in many companies paying into wrong accounts located in different countries in the world which is then nearly impossible to recover.

There are also instances of hackers using sophisticated phishing scheme targeting users having database on the cloud. The tactic allowed attackers to access data stored in the cloud by directing them to the real login page via a malicious link. Those who consider it as real information without understanding the real reason for having such emails sent to them end up forwarding a digital token which gives fraudsters indefinite access to all the cloud data, including emails, files and contacts – even after the victim changes their passwords.

It is important to note that phishing is still the number one cause for data breaches. Bot attacks are sometimes responsible, but still a major data breaches started with phishing techniques. And that's before you even consider other social engineering techniques, which also count as a form of phishing.

There has been trend of phishing techniques from hackers and fraudsters which included creating of fake job posts to access applicants' personal data, and collecting phone numbers for SIM jacking

In 2020, more than ever before especially due to the pace of digitization caused by Covid, companies and individuals need to ensure they are more vigilant at all times to avoid giving away information that could hurt them – especially if they want to avoid embarrassing and reputation-damaging data breaches.

Some of best practices include double confirming via phone call if any payment details are changed on supplier invoices, be extra vigilant for confirmation of financial information over emails, not to click on malicious links sent (always check the exact email ID before clicking any link in the email and unless you are really sure, ask yourself "were you expecting this email?").

3. Open Banking will continue to transform the online landscape

With the continuous improvements and introduction of new methods to further secure the online transactions bought in by Fintechs and established financial institutions will probably create a period of customer confusion. As new services provide OTPs (one time passwords) via SMS, 2FA and MFA, and even more app-based biometric authentication methods, fraudsters will try to exploit the lack of consumer info to fool users into submitting valuable data.

Any periods of change are often fruitful for the fraudsters, as was seen with many implementations of new techniques in the past such as the abuse of Captcha forms.

The new security methods could also impact conversion rates. How to provide a seamless user experience is the new battleground for online businesses, whether it's for onboarding of new customers or for completing transactions. Adding an extra step between customers and their purchases has already proved controversial with certain retailers, for instance when 3DS was rolled out.

On the contrary, banks and fintechs alike are enthusiastic about the new opportunities of open banking. According to FData, 80% of large banks want to support fintechs application development through open banking. Fintechs also welcome the opportunity to scale by partnering with established financial institutions thanks to the brand recognition they will provide.

4. The Asia-Pacific Region Will Need to Curb Fraudulent App Installs

According to a report by AppsFlyer, Asia Pacific was exposed to US$945 million in App Install Fraud in H12020 and Finance apps are the most exposed verticals to fraud. APAC Ad Fraud Report 2019 has revealed that the average fraud rate in the region is 60% higher than the global average.

Based on analysis by AppsFlyer of 2.5 billion installations across 8,000 apps in six consumer segments – entertainment, finance, gaming, e-commerce, travel and utilities – AppsFlyer found around 25 out of every 100 non-organic installs in the region were fraudulent over the six months covered in the report.

So why such high rates in that specific region?
Higher mobile user volumes
High marketeer demand for volume
High rate of fraudulent traffic in local networks
And a trend towards a cost per action (CPA) business model.

The situation was particularly bad in Southeast Asia, where more than US$260m – or 40% of the APAC total – was put at risk.

The good news is that anti-fraud solutions have fantastic track records in reducing bot attacks and install hijacking. So prevention is indeed possible – as long as marketers leverage these solutions efficiently, and fast.

5. Cell phone account fraud

Phone scams is one the major reason for loss of money and sometimes life savings. Scammers have figured out countless ways to cheat you out of your money over the phone. In few cases scammers appears as very friendly willing to help and, in many cases, might threaten or try to scare.

Phone scammers usually try to get either your money or your personal information for identity theft. Below are some of the ways to protect in situations like this,

- **How to Recognize a Phone Scam**

The phone scams can come in many forms, but the process of making promises and threats is quite similar. Some of the ways to identify a phone scam are below.

Pay to get the prize

If someone calls to say that you were "selected" for an offer or you have won a lottery and in order to get the same, a small amount to be paid. Trick clearly shows there is no prize, why will someone ask a payment before giving a prize!

Non-payment can lead to arrestment

Some scammers call to threaten by pretending as calling from law enforcement or a federal agency. They might say you'll be arrested, fined, or deported if you don't pay taxes or some other debt right away. The purpose of such calls is to scare in paying into anything. However, in reality the law enforcement and federal agencies do not call to threaten into payment but will seek a legal course of action.

Forcing to decide on an offer now

If any business offers you a special offer, they will give you enough time to make that decision and will ask for a written confirmation before asking you to commit. So for any urgent offers, always ask for time before committing to it and counter verify with channel or call official landline to confirm before committing to it. Don't get pressured into making a decision on the spot.

There's never a good reason to send cash or pay with a gift card

Scammers will often ask you to pay in a way that makes it hard for you to get your money back – by wiring money, putting money on a gift card, prepaid card or cash reload card, or using a money transfer app. Anyone who asks you to pay that way is a scammer.

Government agencies aren't calling to confirm your sensitive information

Before careful before disclosing any sensitive information like your social security details or personal bank account details etc. Government agencies do no call randomly to confirm such details as they always follow an official channel of doing it. Before providing any such information it is always better to confirm authenticity of caller and also to double confirm the request by contacting such government agency

5. Cell phone account fraud (continued)

Getting sale calls from companies you never heard of

There is a regular phenomenon of people calling to sell new products or to introduce new products, many times they do some basic research before calling so you can expect that they know a bit of history about you. Further with the new machine learning techniques, many times data is bought by companies and this data show the behavior to fall back into.
So be prepared to not give in to sale calls even if that is of interest area, maybe you like to do an independent review before spending.

- **Examples of Common Phone Scams**

Any scam can happen over the phone. But here are some common angles phone scammers like to use:

Imposter scams

Scammer calls and pretends to be someone from the agency that you trust in such as a government agency, a reference from family member, interest, or someone claiming that someone trying to hack into your account. The hackers have become so advanced that it may show as a trustworthy number or a fake name on your caller ID to convince you.

Special relief from debts and final settlement scams

Scammers can offer lower credit card interest rates, ways to fix credit, or ways to get the loans forgiven or waived off, **if you pay their company a fee first**. This is simply a way to use your personal data to fraud you

Offer investment or earn high profits from investment schemes

Callers might promise to help you start your own business stating that they have read your interest areas and very impressed with your business model. This is just a process of enticing you into committing into an investment,
Callers explaining new investment ideas or high profit-making stocks, the purpose is to make you into an investment mode and then recommending them as lead managers. Even going to the extent of giving guarantee for doubling your investment etc.
Just think simply that if they can make so much money then why not putting their own money and if those ideas are so great why they looking for investors!

Introducing as a Charity to make use of your vulnerability

Many scammers simply use the religious authenticity or any big calamity or any cause as a mean to entice people into giving a small portion into charities. They will give background of how much there company has done for the cause and how a small charity can change someone's life etc Always check out a charity before you give, and don't feel pressured to give immediately over the phone before you do.

5. Cell phone account fraud (continued)

Extended vehicle guarantees
Tricksters discover what sort of vehicle you drive and when you got it so they can encourage you to purchase overrated – or useless – administration contracts.

"Free" trial for products
A caller may call offering free trial of a new product and let you sign into product purchases without informing properly about the conditions attached to the free trial.

Loan scams
Scammers are good at tracking history of customers with bad credit history and they can anticipate that they will still be looking for more loans. They call such people offering their service in raising fresh loans or arranging to write off old loans for a fee to be paid in advance, sometimes such fee is so low that people can take the risk of a big advantage attached to it.

Prize and lottery tricks
In a regular prize trick, the guest will say you've won a prize, yet then state you need to pay an enlistment or transportation expense to get it. Be that as it may, after you pay, you discover there is no prize.

Travel and timeshare scams
Fraudsters promise low cost vacations and even free by stating that you are one of the selected person out of a draw, they will not discuss about the hidden costs which eventually mean that you might end up paying more than what would have costed buying a more straight forward deal. They will ask for early commitment or to book the timeshare by paying a small fee.

- **How to Stop Calls from Scammers**

Drop the call
If you sense during the call that it is leading you into a scam, just simply hang-up. Sometimes robocalls are also made to introduce a product, do not press any numbers, just hang up.

Consider call blocking or call labeling
Most of the scam calling is done using internet calling systems. The easiest defense against such calling is doing a call blocking. Once you know that a call was a scam call, it is better to block such number so they cannot reach you again.

Do not rely on your caller ID
Hackers and scammers are normally well versed with latest technology and they have most advanced means to get into systems of people, Thus scammers can make any name or number show up on your caller ID. That's called spoofing. So even if it looks like it's a government agency like the Social Security Administration calling, or like the call is from a local number, it could be a scammer calling from anywhere in the world.

5. Cell phone account fraud (continued)

- **What to Do If You Already Paid a Scammer**

The method selected by scammers is such that it is always difficult to get the money back and most of its impossible to catch the scammer since they are well prepared for such acts.

In case your credit card is used for such payments, always make a dispute committee of the bank, there is a higher chance that they will reverse it since controlling scammers is one of the mandates of the bank as well. The moment you have a fraud charge on your card, call the bank customer care to block your card as the more delay it takes there is chance that more wrongfully it could be used

On the off chance that you paid a scammer with a credit card, you might have the option to stop the exchange. Contact your credit card organization or bank immediately. Mention to them what occurred, and request a "chargeback" of the charges.

In case you have paid the scammer with a gift voucher, pre-loaded card, contact the organization that gave the card immediately. Reveal to them you paid a scammer with the card, and inquire as to whether they can discount your cash or a way to stop usage of it. The sooner you get in touch with them, the better it is

In the event that you paid the scammer with an online wire transfer, call the bank quickly to report the misrepresentation and record an objection. Call the dispute division:

On the off chance that you gave the scammer access to your PC, update your PC's security immediately. Always run a high security check and speak to some of your IT friends for advice on this matter.

In the event that you gave your username and password to the scammer, change your secret key immediately. In the event that you utilize similar secret key for different records or destinations, change it there, as well. Make another secret word that is unique.

In the event that somebody calls and offers to "help" you recuperate cash you have just lost, don't give them cash or individual data. You're likely facing another trick from scammers, always reach out to authenticated sources to report.

6. WhatsApp fraud and how do you prevent it?

Do you know whatsApp users at end of February 2020 were over 2 billion? Because of its size and accessibility, it has become irresistible platform for fraudsters.

During the first six months of 2020, the frauds carried out through WhatsApp were on rise and yet with very level of prosecution. So lets understand different kinds of frauds conducted through whatsapp,

- **Friend or family emergency scam**

A greater part of fraudsters act like a friend or a relative and request monetary assistance since "they critically need to pay a (high) bill" or "they have a crisis and direly need some cash".

They create so much of rush that do not allow reaction time. The average loss of money is in thousands of dollars and most of victims are over 50 years of age.

By and large the telephone number utilized by the criminal to perpetrate WhatsApp misrepresentation is not known to the person in question, yet the profile picture is real. Further, the tone of approach makes the person believe it is undoubtedly speaking with a companion or relative. Fraudsters can without much of problem can download the photograph from other social media channels such as Facebook or Instagram.

- **WhatsApp hijacking**

This is a system when the fraudsters actually breaks into the actual account and approach family members for help. The below scenario looks highly unlikely but happens more often than you can imagine,

→ Scammer identifies the victim and get hold of his number most widely used on whatsapp
→ This person than install another whatsapp application on his phone or his/her computer device
→ This fraudster than approach the target victim by appearing as a colleague or a friend and saying that he/she is using a different number to contact as he is facing some issues with his original number.
→ The scammer than says that he/she was reinstalling the whatspp and by mistake has given the victim's number due to which a verification code might have come and requesting to provide the same.
→ The cybercriminal fools the victim into giving them the confirmation code, which they at that point type it into their own telephone hence accessing the victim's WhatsApp record and all the victim's contacts.

6. WhatsApp fraud and how do you prevent it? (continued)

- **Voicemail box hijacking**

Another regular trick to access a victim's WhatsApp account includes breaking into a victim's voice message box to take the WhatsApp verification code. At the point when WhatsApp is (re)installed, the application sends an instant message to the predetermined telephone number with the verification code. Nonetheless, the cybercriminal can demonstrate that he/she has not gotten the code and request to get a call all things considered, realizing that WhatsApp will call the casualty in no time. The fraudster will at that point call the casualty's telephone number at the very same time. Since the casualty is on the telephone, the confirmation code is then sent to the victim's phone message box.

- **How to prevent against a whatsapp fraud**

Some easy tips to identify a whatsapp fraud and to prevent against are as below,

→ In the event that you get a message from somebody who is requesting cash, first check whether the number is right. In the event that one of your companions or associates unexpectedly has another number and approaches you for cash, you should get suspicious!

→ Briefly stop and check the language and correspondence style of the message. Is it unique/more regrettable than expected? Assuming this is the case, there is a reasonable possibility you are managing a WhatsApp trick

→ Attempt to call the person requesting cash. In the event that it is a trickster, they will likely be immediately uncovered!

→ On the off chance that the fraudster does not pick the phone, attempt to call the "old" number you have for your companion or associate, or reach them in an alternate way (for example email, SMS, and so forth) to confirm the story

→ Try not to let the fraudster pressure you. Think consistently and resist the urge to panic. In the event that somebody approaches you for cash to cover a pressing obligation with, for example, an energy provider or government organization, ask yourself how probably is that a couple of hours postponement would matter.

→ In the event that you are in doubt, try to say something for which a peculiar response is expected that can help you gauge the originality of the person contacting.

→ Secure your phone message with an unique code that lone you would know. This makes it more hard for WhatsApp fraudsters to get to your phone message box to recover a WhatsApp confirmation code.

6. WhatsApp fraud and how do you prevent it? (continued)

→ On the off chance that somebody requests that you send a verification code, never send it if in doubt or not expecting. Continuously look for contact with the individual you think you are conversing with in an alternate manner. The above is significant if the individual mentioning the confirmation code is not a very common friend. Remember that if an individual necessities a verification code, they could just demand it again from WhatsApp as opposed to reaching you.

→ Set up "2-Factor Authentication" on WhatsApp. When this is setup, if introducing WhatsApp on another gadget, WhatsApp will demand the 6-digit code you have set just as the confirmation they send you. This will make account capturing substantially more hard to accomplish.

7. Air-ticket fraud

Not all flight tickets fly !

That's because scammers are trying to take advantage of the ongoing pandemic and might target you with fake confirmed flight tickets on repatriation flights or chartered flights. They might create a sense of urgency to make you pay through account transfer or credit card. They might even email you a fake ticket before becoming untraceable. But all is not lost. Here's how to stay safe from ticketing frauds.

Stay safe from ticketing frauds:

→ Always check any flight ticket offer with the concerned airlines/ authority, before making any payment
→ Do not share any personal banking/ credit card information
→ Please be cautious and fact check all COVID-19 related social media posts, SMS and calls

Premier Brains
Accounting + Auditing

UPDATE

HOW PREMIER BRAINS CAN HELP?

Premier Brains has a team of experts who have strong background in forensic audits. You can consult us on setting up systems to protect against fraud risks and to be aware of new ways to secure your systems and your privacy.

We know technology is taking us forward but fraudsters are using the same technology to take us backwards, so let's be aware and let's take the right precautions!

Reach out to our partner in charge of forensic audits rishi@premier-brains.com for more information and you may call us at +971 4 354 2959

"ALWAYS DOING THE RIGHT THING"

ABOUT PB Premier Brains is a firm of qualified and experienced audit, tax and finance advisors. Delivering exceptional business value to our clients is our primary goal.	• Audit and Assurance (External & Internal) • Tax Agency with FTA • Tax Advisory • Business valuations • Feasibility Studies • Business Accounts Outsourcing Services	• Fund raising and restructuring • JAFZA Offshore agents • Company incorporations (under group entities)