LEGAL UPDATE

ASSET RECOVERY UPDATE

15 October 2019

REMEDIES FOR DIGITAL FRAUD

SUMMARY

Online services have become an integral and increasingly important aspect of daily life. However, the importance and value of digital assets also means that cybersecurity and the prevention of digital fraud becomes a critical concern, for both individuals and businesses.

Some knowledge of how digital fraud operates can help one to avoid becoming a victim. This article explains some common digital fraud techniques and methods, and the potential legal issues.

INTRODUCTION

Our modern lives are intertwined with technology. Email is ubiquitous, social media is omnipresent, our digital possessions (including software or audio-visual media) are tied to online accounts, and we store our private and personal information online via cloud storage platforms. The increased value of our digital assets creates an incentive for malicious third parties to try to steal these assets.

Despite this risk, we often do not do enough to protect our digital assets.

This article touches on some methods of digital fraud, and the remedies that may be available to a victim. As digital fraud can be a complex technical field, we summarise the concepts in simple terms below.

Phishing or email spoofing

Some fraudsters send fake emails, pretending to be someone else. This can range from the common but relatively unsophisticated scams involving purported inheritance or foreign royalty, to specific and targeted attempts to compromise a company by impersonating a customer or officer of the company.

In phishing, the fraudster sends an email from a fake email address that is designed to look legitimate. There are many potential methods. The email could be obviously fake with a completely different email address, or a different but similar looking email address, or even appear to be an entirely legitimate email from a real email address via a process known as “spoofing”.

This should be of concern for businesses. A fraudster might attempt to compromise a company’s junior staff by sending a fake email ostensibly from the company CEO or other senior executive. In such a situation, the junior staff member might not even consider questioning the authenticity of his superiors’ instructions. It is easy to understand why a junior staff member (for example an accounts clerk) might not want to call his CEO to check whether the CEO truly sent an email requesting for certain information or documents.

Fake websites containing malicious code

In parallel with fake emails, fraudsters may create fake websites. A fake email could induce a user to click through to a fake website, to trick the user into entering their login and password details.

These websites can be dangerous even if the user is savvy enough to know not to enter any sensitive data or download any files. The website itself could contain malicious code, to exploit system vulnerabilities and run malicious code or download malware without the user’s knowledge.

Malware

Malware (*ie* malicious software) is a general term used to describe software designed to damage or affect a computer. A phishing email or fake website can be used to surreptitiously download malware into a victim’s computer.

Depending on the type of malware, this can be used to steal data or information, monitor the user’s activities, or possibly lock down the victim’s computer entirely (known as “ransomware”). Malware can also be used to hijack the victim’s

computer, and possibly to lay in wait for an opportune moment to reap the fruits of fraud.

Leaked password data

Many services now require an online account of some kind. Given the sheer number of online services we use in our daily lives, it can be difficult to remember a unique password for every different service.

Many of us therefore opt for the convenient route of re-using passwords, which increases the risk that a security breach at one website will compromise a user's other accounts. This is especially if the leaked passwords are subsequently sold or traded online.

COMMENTARY

Victims of digital fraud, like victims of any kind of fraud, would usually benefit from seeking legal advice without delay. Identifying the breach and working on possible solutions in a timely manner can help mitigate loss, and also increase the possibility of recovery by potentially locating the perpetrator before they vanish and wipe their presence.

Where the hack has compromised an online account, the victims should also change their passwords for any other online accounts that use the same password.

Where a fraudster manages to secure access to a user's bank account or financial information, he might still need time to withdraw the money, transfer funds out of jurisdiction, or make fraudulent purchases. A prudent first step for any compromised user would be to contact his bank or card issuer to ensure that they are aware of possible fraudulent transactions, so that they can stop these transactions or stop fund transfers out of the user's bank account.

If the wrongdoer cannot be identified, it may be possible to seek an order under Order 24 Rule 6(5) of the Rules of Court for discovery of documents against a non-party (such as the recipient bank) for the purpose of identifying the ultimate fraudster as a possible party to proceedings. This could also fall under the Court's overlapping jurisdiction to order production of such documents based on the principle in *Norwich Pharmacal Co v Customs and Excise Commissioners* [1974] AC 133.

In parallel, it may also be possible to seek disclosure of documents to assist with efforts to trace any misappropriated funds, by way of a "Bankers Trust" order (named after the English Court of Appeal's decision in *Bankers Trust Co v Shapira* [1980] 1 WLR 1274).

Where data or information has been compromised, steps can be taken to prevent further leaks, and to identify where the data might have been transferred. Court proceedings can be brought if the attacker can be identified, and it may be possible to seek injunctions to prevent use or further dissemination of misappropriated data.

From the organisation's perspective, under the *Personal Data Protection Act 2012* (No 26 of 2012) ("**PDPA**"), an organisation might be liable for failing to protect personal data. Section 24 of the PDPA requires an organisation to make reasonable security arrangements to prevent unauthorised access among other things.

In [2019] SGPDPC 3, which involved Singapore Health Services Pte Ltd ("**SingHealth**"), a hacker had gained access to a workstation via an email phishing attack. The hacker then used various tools to access a Citrix server, among other things, and a database of personal data. The Commission considered the security measures implemented by SingHealth but ultimately held that SingHealth had breached its obligation under Section 24 of the PDPA, because it had not taken sufficient security measures to protect personal data from unauthorised access and illegal copying. SingHealth was directed to pay a financial penalty of S$250,000.

Apart from seeking civil remedies, victims of digital fraud can also lodge police reports. Acts of hacking are criminalised in Singapore under the *Computer Misuse Act* (Cap 50A) ("**CMA**"). Under the CMA, it is an offence to knowingly cause a computer to perform a function, or to secure access without authority to any program or data in a computer. It is also an offence to modify the contents of a computer without authority, or to use or intercept computer services without authority. Phishing may also constitute the offence of cheating under the *Penal Code* (Cap 224).

Criminal investigation by the state can potentially identify an otherwise unknown fraudster, but

victims would likely still need to commence their own civil claims to recover stolen assets and property if the fraudster does not voluntarily make restitution.

Businesses and individuals expose themselves to digital fraud when an attacker can exploit vulnerabilities or weaknesses in their security infrastructure, or take advantage of individual users being lax with cybersecurity. To best protect themselves from digital fraud, businesses and individuals should always exercise care, and should at the very least be aware of what to look out for.

If you have any questions or comments on this article, please contact:

Gary Low
Director, Dispute Resolution
T: +65 6531 2497
E: gary.low@drewnapier.com

Click here to view Gary's profile

Terence Tan
Associate Director, Dispute Resolution
T: +65 6531 2378
E: terence.tan@drewnapier.com

Click here to view Terence's profile

Click here to learn about our **Commercial Litigation Practice**

Click here to learn about our **Asset Recovery Practice**

LEGAL UPDATE

Drew & Napier LLC
10 Collyer Quay
#10-01 Ocean Financial Centre
Singapore 049315

www.drewnapier.com

T : +65 6535 0733
T : +65 9726 0573 (After Hours)
F : +65 6535 4906