Government of Western Australia
Department of Commerce

Real Estate Industry e-Bulletin

An electronic bulletin from the Consumer Protection Division of the Department of Commerce

Issue 26 **18 October 2012**

Weblinks

CPD Information

Newsletter Archive

e-Bulletin Archive

Departmental Publications

Contact Us

Privacy Statement

Copyright

Unauthorised phone porting used to steal funds

Consumer Protection would like to advise real estate and settlement agents of a sophisticated 'porting' scam which could have serious implications for you.

It appears fraudsters are increasingly trying to steal mobile phone numbers to intercept online banking verification codes. This allows the fraudsters to use unauthorised SIM porting to illegally transfer funds from bank accounts and this could be a very real threat to an agent's trust account.

Porting is the act of transferring a mobile phone number to a new service, either with a different network or a different provider, or both.

Consumer Protection is aware of a recent case where unauthorised porting has been used to divert payments from an agent's trust account.

Typically during the first stage of the scam, fraudsters will compromise a victim's computer system in order to access their banking and trust account details (eg user name, password, trust account number etc.). There are several ways computer systems can be compromised and while no specific method has been identified in this particular scam, it appears that banking details may have been stolen when the agent conducted an online banking session (the fraudster may have been able to bypass inadequate security software).

Once a fraudster has an agent's banking and trust account details, they can arrange to transfer funds to their own bank accounts which are often located overseas. The offshore location limits the Federal Police's ability to track and recover the funds.

Most major banks have SMS verification systems which send online banking users SMS messages before allowing them to transfer large amounts of money to unfamiliar accounts. When a new, large or unorthodox transaction is attempted online, the bank sends a verification code to the account holder's mobile number as an additional authentication measure. The account holder then types the code and sends it back to the bank which then processes the transfer.

Fraudsters bypass this security process by porting the original mobile number to a number they now control. The bank's SMS goes to the fraudster's mobile number rather than the account holder's number. The fraudster then enters the verification code which authorises the transfer of funds.

...continued on page 2

Government of Western Australia
Department of Commerce

Real Estate Industry e-Bulletin

An electronic bulletin from the Consumer Protection Division of the Department of Commerce

continued from page one

Mobile number portability is regulated under an industry code. The code, amongst other things, requires a phone provider's call centre representative to ask questions to ensure a customer has authorised the porting process (eg a customer number and date of birth).

It appears fraudsters steal people's customer number and date of birth by accessing online bills, bank accounts and personal or professional documents (remembering they have compromised the victim's computer). They may also call the person and ask identity questions by posing as legitimate businesses. Fraudsters may also use social media such as Facebook to gather personal details.

The fraudsters use this information to call the victim's mobile phone provider and ask for the phone number to be ported to a new device. Some fraudsters even pose as the victim's mobile phone provider and send a text saying there are network difficulties and that there may be problems with mobile reception for the next 24 hours. This gives the fraudsters time to commit the scam.

The porting scam summarised for agents

When fraudsters have all parts of the scam in place, they can access an agent's bank account(s) via online banking and arrange to transfer large sums to their own account. The agent's bank SMS verification system detects the 'unusual' transfer and sends the account holder's registered mobile phone number a verification SMS. The agent never receives the SMS, as their number, via porting, is now on the fraudster's mobile device. The fraudster responds to the SMS by entering the code the bank supplies. This authenticates the transaction and allows the fraudsters to access the stolen trust account funds. The agent is none-the-wiser and it may take some time before the trust account fraud is detected. Additionally, the agent no longer receives calls as their mobile number has been diverted.

Trust Account Implications

Generally, when any shortfall or deficiency is identified in an agent's trust account, the agent should as standard practice immediately remedy the shortfall by transferring funds from the trading account or, where this is not possible, from personal funds.

For further advice in remedying any shortfall in a trust account, it is suggested the agent should, in the first instance, seek advice from their statutory appointed auditor, followed by Consumer Protection.

It is important to note that fraudsters may attempt to access either your business or personal accounts.

...continued on page 3

Government of Western Australia
Department of Commerce

Real Estate Industry e-Bulletin

An electronic bulletin from the Consumer Protection Division of the Department of Commerce

continued from page two

What to do if you have been scammed

- Contact your bank or credit union immediately so they can investigate the suspect transaction, suspend your account and take appropriate action.
- If you have been scammed of money, report the crime to the local police.
- If you have a shortfall in your trust account, seek advice from your statutory appointed auditor, followed by Consumer Protection.
- Report ID fraud scams to ScamNet via email on scamquery@commerce.wa.gov.au or call the Consumer Protection advice line on 1300 30 40 54.

How can I protect myself?

The following tips should help secure your identity and avoid SIM porting.

- Call your mobile network provider and insist that additional security questions be added to your account before your number can be ported. Try to add questions which may not be readily answered by fraudsters.
- Ensure all the online devices you use have up-to-date security software. This includes your personal and work systems.

Real estate agents and settlement agents should also regularly check resources available from industry bodies such as Telstra, the Communications Alliance and the Australian Communications and Media Authority. The following link provides valuable information on unauthorised phone porting and identity theft: Telstra.