

COMMISSIONER'S BULLETIN



DEPARTMENT OF CORPORATIONS Supporting a Fair and Secure Financial Services Marketplace for all Californians

www.corp.ca.gov

Edmund G. Brown Jr.
Governor

Jan Lynn Owen
California Corporations Commissioner

DATE: May 21, 2013

Commissioner's Bulletin No. 002-13

Protecting Escrow Trust Accounts From Cyber-Hacking

You are being sent this urgent bulletin to alert you of the growing threat of cyber-hacking of escrow trust accounts.

The Department of Corporations has been informed of two escrow companies who were the victims of cyber-hacking this year, together losing an estimated \$2,000,000 in trust funds. Both cases involved unauthorized wires to foreign bank accounts. One company took extraordinary efforts to replace the funds and is still in business. The other company was not able to replace the funds and is currently in conservatorship. This is an important reminder that each escrow agent must be vigilant in protecting trust accounts.

Though the alleged cyber-hacking cases are still under investigation, a common issue appears to be malware and computer viruses infecting the computers. These viruses can copy keystrokes and obtain passwords, which are sent to cyber-hackers all over the world.

In at least one case, it appears that the hacker took control of the escrow agent's computer after the agent typed in a secure token number to access the trust account.

What You Can Do

Escrow companies' paramount duty is to protect consumer funds by managing the trust accounts in a safe and sound manner. An important step in meeting that obligation is being proactive about understanding the protections offered by your bank. Escrow agents should thoroughly review security measures with the bank and ask questions of their banker to ensure that they are using the most secure protections available.

Another protection suggested by bankers is to dedicate a single computer to be exclusively linked to trust accounts so that no other business occurs on that computer or through its

Internet connection. This practice makes it less likely that viruses will be caught by visiting questionable websites. Companies should also ensure that their computers are properly protected with up-to-date antivirus software.

Another important protection is ensuring you reconcile trust accounts promptly. All adjustments should be researched and corrected on at least a monthly basis. In the two incidents noted above, this was the ultimate factor in determining whether the company remained in business or not. Interest-bearing accounts must also be monitored.

Escrow agents should also consider insurance coverage for trust account losses due to cyber-hacking or other unauthorized access. It is important to note that losses of this nature are not covered by Escrow Agent's Fidelity Corporation (EAFC). Refer to Financial Code Section 17304 for the definition of losses covered by EAFC.

If a trust account shortage occurs, no matter the cause, you should immediately report it to the Department of Corporations and EAFC. Shortages must be immediately replaced. An escrow agent will lose licensure if a trust account is not restored to its proper balance.

Should you have any questions, please contact Kathleen Partin, Special Administrator for the Department's Escrow Unit at (213) 576-7595.