

DEPARTMENT OF BUSINESS OVERSIGHT*Ensuring a Fair and Secure Financial Services Marketplace for all Californians*

Jan Lynn Owen
Commissioner of Business Oversight

April 29, 2016

IN REPLY REFER TO
FILE NO:

Protecting Escrow Trust Accounts from Cyber-Hacking

Commissioner's Brief

The Department of Business Oversight (DBO) has received reports of cyber-hacking of escrow trust accounts every month for the past nine months. More than \$1.5 million dollars has been redirected by hackers with fake email wiring instructions. Hackers have successfully accessed email accounts of principals, real estate agents and escrow companies.

The most common attack method is the "phishing" email. The hacker sends an email that appears to be from a lender, real estate agent or someone wanting to open an escrow. The email contains a link that is supposed to provide loan documents, real estate contracts or other information. Once the link is opened, malware infects the escrow agent's email system. The hacker then is able to read and see all incoming and outgoing emails and alter them when funds are about to be sent. They also have access to any forms, instructions, signatures, etc., that are sent by email. Hackers have even duplicated a bank's wire receipt confirmation telling the escrow agent that incoming funds were in their account, when they were not.

What You Can Do

An escrow agent's number one duty is to protect consumer funds by managing the trust account in a safe and sound manner. You must proactively train your staff to recognize the "red flags" of cyber-attack. Never accept an emailed instruction that changes the original funding instructions. Documents sent by email can be altered easily and true signatures scanned to make them look legitimate. Know your principals, telephone your clients and confirm their identify. Never call the number in an email, as you could be talking to the hacker.

1515 K Street, Suite 200
Sacramento, CA 95814-4052
(916) 445-2705

One Sansome Street, Suite 600
San Francisco, CA 94104-4428
(415) 972-8565

320 West 4th Street, Suite 750
Los Angeles, CA 90013-2344
(213) 576-7500

1350 Front Street, Room 2034
San Diego, CA 92101-3697
(619) 525-4233

45 Fremont Street, Suite 1700
San Francisco, CA 94105
(415) 263-8500

300 S. Spring Street, Suite 15513
Los Angeles, CA 90013
(213) 897-2085

7575 Metropolitan Drive, Suite 108
San Diego, CA 92108
(619) 682-7227

You must take proactive steps to protect your company from attack. Speak with your CPA, banker, and IT person about internal controls. Consult with your trade associations. Make sure your software is up to date and free of malware. Companies that balance their trust account daily have done well in recovering lost funds, as timely discovery and quick wire recalls can be successful. The Escrow Institute of California recently issued a blast email alert on the latest scams and ways to combat them. Recent articles by the Federal Trade Commission and National Association of Realtors discussed this increasing threat to all parties in the real estate business. View their websites for additional information.

As a licensed escrow agent, you also have certain legal requirements if you become a victim. California Financial Code section 17414 requires that you report in writing any such incident *immediately* to the DBO and EAFC. Any missing trust funds must be promptly replaced by the company, as debit balances are prohibited (Title 10, California Code of Regulations section 1738.1). EAFC does not cover this type of loss. Private insurance is available, but be aware of coverage limitations. The DBO will conduct an investigation of each incident to see if the company acted according to their *signed* instructions and whether the disbursements were done in a reckless manner. A licensee may be subject to administrative action, including a desist and refrain order, and suspension or revocation of license.

The actions you take now will not only safeguard your customer's trust funds, but save you from severe financial loss or even the potential failure of your company.