FRANZEN & FRANZEN, LLP
CERTIFIED PUBLIC ACCOUNTANTS

February 8, 2013 – Identity Theft and Taxes

Across the nation, identity thieves are using legitimate information to scam honest taxpayers, and frequently posing as a representative from the IRS or a state tax authority to do so. The IRS and Franchise Tax Board are taking this problem very seriously. Being aware of some of the most common scams can help protect you from having your personal information used to commit fraud or other crimes.

Phony emails. In a "phishing" scam, an official-looking email shows an IRS or FTB logo that lures the consumer to a website that requests personal and financial information, such as a Social Security number, bank account, or credit card numbers. In truth, neither the IRS nor the FTB will initiate contact with a taxpayer via email. They do not send out unsolicited emails to ask for detailed personal or financial information such as PIN numbers, passwords or similar secret access information for credit cards or bank accounts.

Refund scam. In a refund scam, a bogus email tells the recipient that he or she is eligible to receive a tax refund for a given amount and sends the recipient to a website to complete a form to submit the tax refund request. The form then asks for personal and financial information. Once again, the IRS and FTB will not notify taxpayers of refunds via email. Taxpayers will not be asked to complete a special form or provide detailed financial information to obtain a refund. Refunds are based on information reported on their tax returns.

Antifraud Commission scam. In this case, the scammer sends an email stating the IRS "Antifraud Commission" has found that someone tried to pay their taxes through the Electronic Federal Tax Payment System, or EFTPS, using the email recipient's credit card and, as a result, some of the recipient's money was lost and the remaining funds were blocked. The email includes a link that sends the recipient to a website where he or she is directed to enter personal and financial information in order to unblock their funds. Don't take the bait! The IRS does not have an Antifraud Commission and does not have the authority to freeze a taxpayer's credit card or bank account because of potential theft or fraud perpetrated against the taxpayer, and does not use email to initiate contact with taxpayers.
Other email scams from fraudsters posing as IRS or FTB personnel include notifications of lottery winnings, a notice that more than one return was filed by the taxpayer, and notification of W-2s received from an unknown employer. Scams can also take the form of "assisting" taxpayers in filing returns to collect fraudulent refunds, promotion of tax evasion techniques, or reporting false income for purposes of increasing refundable credits.

Get help. Both the IRS and the FTB have created Identity Theft Units to address the growing problem of fraudulent identity. A taxpayer who believes there is a risk of identity theft due to lost or stolen personal information should contact the IRS and/or the FTB immediately so the agencies can take action to secure his or her tax account. The taxpayer should contact the IRS Identity Protection Specialized Unit at (800) 908-4490 and the FTB ID Theft Resolution Coordinator at (916) 845-3669.

For more information, visit the IRS website www.irs.gov or the FTB website www.ftb.ca.gov. We also encourage you to contact our office, particularly if you believe your identity may have been fraudulently compromised.