IRS and Identity Theft and Scams

A. Most recent large scam:

1. Robo calls impersonating U.S. law enforcement and telling taxpayers that they need to contact the callers immediately to avoid arrest and criminal prosecution for tax non-compliance. Victims are asked to make a payment using prepaid cards.
2. TIGTA: as of July 2015, at least 9,000 to 12,000 new cases were reported each week; over 3,900 victims have been identified with a total of over $20 million in financial losses.
3. In 2015, one Sahil Patel was sentenced to 14 years in prison and $1 million in forfeitures for running a "massive" fraud ring through call centers in India. Mumbai crackdown in 2016.

See page 1-236

IRS and Identity Theft and Scams

A. Practitioner scam announced in IR-2017-3:

1. Cyber criminals contact a practitioner by email in two stages.
   a. In the first email, the criminal claims to need a preparer. If the preparer responds, a second email is sent that typically contains either an embedded web address or a PDF attachment that has an embedded web address.
   b. The preparer may think he or she is downloading a potential client's tax information or accessing a site with such tax information. Instead the criminal is collecting the preparer's email address and password, and possibly other information.
2. IRS: Preparers should develop policies on how to address unsolicited emails seeking their services.

See page 1-238

IRS and Identity Theft and Scams

A. Another practitioner scam announced in IR-2017-111:

1. Criminals send an email to preparers purporting to be from a tax software education provider.
    a. The information sought will allow the thief to steal client data and file fraudulent returns by getting e-Service credentials.
    b. The IRS announcement contains a sample phishing email. It begins: "In our database there is a failure, we need your information about your account." It then asks for a copy of a driver's license, as well as information such as e-Service usernames, passwords, and PINs, as well as EINs and "Mother's Maiden Name."
2. Report such an email to **phishing@irs.gov.**

See page 1-238

IRS and Identity Theft and Scams

A. A variation scam announced in IR-2017-126:

1. Cybercriminals impersonate tax software providers and send an email with the subject line "Software Support Update."
    a. The email provides a link to a fictitious website that mimics the software provider's actual login page.
    b. Instead of upgrading software, the tax professionals are providing their information to criminals who use the stolen information to access the preparers' accounts and steal client information.

See page 1-238