

ABA Meeting: No Easy Fix for Increasing Theft of Employer Identification Numbers

by Jeremiah Coder

Full Text Published by **taxanalysts**[®]

Thefts of employer identification numbers are increasing, but the IRS offers few solutions to affected businesses, according to panelists who spoke at an Administrative Practice session of the American Bar Association Section of Taxation meeting in Washington on May 10.

EINs appear on many public documents, including SEC filings and Forms W-2, and in public database information, and so are easy targets for fraudulent schemes, said Maxine Aaronson, a Dallas-based attorney. IRS e-filing acknowledgement requirements also list preparer tax identification numbers, EINs, and electronic filing identification numbers. Given that the government can match a PTIN to other data, "why isn't a PTIN simply enough -- why are we broadcasting all this information?" Aaronson asked. (Prior coverage )

National Taxpayer Advocate Nina Olson said it was a good question, because the PTIN database is linked to applicable EINs. "There shouldn't be any need for an EIN," but one reason to require it is to show where a preparer is working, Olson said.

Aaronson said there's little business taxpayers can do if they believe their EINs have been stolen. Olson acknowledged that there is no direct way to report a stolen EIN to the IRS and said procedures should be developed. Olson noted that many businesses will send a letter to a customer's prior address to prevent fraud when an information change occurs and said it should be a simple matter for the IRS to do the same when the address associated with an EIN changes. "I hope that the IRS will agree to do that," she said.

Taxpayers who use third-party payroll processors should regularly examine their tax accounts to ensure that payments are properly being made to the government, Olson said.

W-2 Fraud

Phony Forms W-2 result in about \$5.2 billion of fraudulent income tax returns annually, according to Debera Salam of Ernst & Young LLP. The business taxpayer is responsible for any problems associated with fraudulent refunds or missed tax payments, Salam said. Large employers are particularly susceptible to fraud because it can be difficult to identify bogus forms when dealing with large numbers of employees. The IRS doesn't match Social Security numbers on Forms W-2 with the Social Security Administration until after the tax year ends, so notices generally won't be sent until at least a year after the fraudulent return filing, she said.

The IRS has begun a process to allow large employers to submit data from Forms W-2 early in the filing season so the information can be matched with income tax returns, Salam said. However, that process has not been widely promoted and employers can't enroll without an invitation from the IRS, she said.

Olson said the voluntary early matching process is done manually and suffers from the general strain on resources under current IRS funding. In annual reports to Congress, the Taxpayer Advocacy Panel has suggested delaying return processing until all information has been received so that data across documents can be matched comprehensively, she said.

Proposed Solutions

Several proposals in President Obama's fiscal 2014 budget would help fight EIN theft, including giving the IRS access to wage information reported in the National Directory of New Hires, Salam said. However, many proposals, such as applying civil penalties and truncating SSNs on forms, wouldn't address problems with EINs, she said. Requiring employers with more than 50 Forms W-2 to file them electronically would also allow the IRS to match data faster, she said.