Managing Third-Party Risk Key To IRS E-Authentication Proposal

By Luca Gattoni-Celli — luca.gattoni-celli@taxanalysts.org

An IRS proposal to refer to contact information held by third parties for authenticating filers' identities entails distinctive risks and considerable logistical challenges, information technology security experts told Tax Analysts.

The IRS is billing e-authentication as a way to ensure "secure digital interactions with taxpayers" so it can eventually introduce fully featured online taxpayer accounts as part of its "future state" vision announced earlier this year. (Prior coverage: *Tax Notes*, Feb. 29, 2016, p. 974.)

But businesses struggle to manage their own client lists, making a contact list encompassing all taxpayers "orders of magnitude larger," said Dunbar Security Solutions Chief Operating Officer Christopher Ensey, who added that "the demographics present unique challenges to data quality management."

Given its recent struggles with identity theft, the IRS should in general be cautious about how it increases automated access to taxpayer information, said Marcus A. Christian of Mayer Brown LLP.

> ***'There are not always simple solutions to issues in this rapidly evolving area involving cybersecurity,' the IRS said.***

"There are not always simple solutions to issues in this rapidly evolving area involving cybersecurity," the IRS told Tax Analysts in a statement. "In this limited budget environment, we are striving to maximize access to online services while maintaining strong security protocols."

IRS Confirms Spring Target

The IRS — in a document labeled as a January 11 presentation by Commissioner John Koskinen to congressional staff — proposed its new e-authentication process to verify the identities of filers transacting online with the IRS, starting with the restoration of full online access to the Get Transcript tax record application as early as spring 2016.

Having previously downplayed that timeline, the IRS confirmed to Tax Analysts that it is working to restore online access to Get Transcript "later this spring with enhanced taxpayer-identity authentication techniques that will not rely solely on IRS information like" Social Security numbers and dates of birth.

The IRS said it would not discuss specific aspects of its underlying protocols and systems for security reasons but added that the enhanced security protection and authentication methods will be thoroughly tested to validate them before online access to Get Transcript is restored.

E-authentication is referred to in multiple IRS documents outlining its future state vision, a modernization effort to move most filer services online. (Prior coverage: *Tax Notes*, Feb. 22, 2016, p. 847.)

The January 11 slide show describes the IRS's future state vision for authentication: "We will leverage third party contact data that will allow us to send a unique identifier to a taxpayer in real-time." That description implies that the IRS will use records of filers' phone numbers or email addresses supplied by a third party to send them a confirmation code, a common method of multifactor authentication.

'A Massive Endeavor'

U.S. citizens and residents often have multiple email addresses and phone numbers, which may change as they change jobs or homes, Ensey said, adding that he would expect the migration of phone customers from landlines to mobile devices to produce "constant data churn" in the taxpayer contact database.

Ensey said the records of credit reporting agencies, a plausible third-party source for independently verified contact information, are riddled with inaccuracies and duplications. He cited a 2013 Federal Trade Commission study that found one in five consumers had an error on at least one of their three credit reports.

> ***The records of credit reporting agencies are riddled with inaccuracies and duplications, Ensey said.***

Therefore, the IRS's third-party partner will have to create a system for millions of filers to update their own contact information. That would be "a massive endeavor," but "the greater risk is that the system is so easy to use and efficient that hackers can exploit it," Ensey said.

To update her own contact information, a filer would verify her identity using other information, likely some kind of knowledge, Ensey said. "Many of us have already been victims of identity theft," so the information realistically needed to maintain the contact database's accuracy may already be available on the black market, he said.

"At this point, it's premature to speculate that our security protocols are flawed before the enhanced program is launched," the IRS said. "Speculation now is based on an incomplete picture of the process we will put in place."

The Weakest Link

Before joining Mayer Brown in 2013, Christian was the third ranking official in the U.S. attorney's office for the Southern District of Florida. Christian indicated that working with prosecutors in southern Florida, which he noted was an epicenter of tax fraud, gave him a sense that although the IRS detects and prevents significant fraud, identity thieves may still be stealing billions of dollars each year without ever being caught.

Christian emphasized the inherent risks the IRS would face contracting with a third party. As an illustration, he said sizable portions of the National Institute of Standards and Technology's IT security guidelines for federal agencies concern partnerships with outside venders, outlining due diligence standards that include reviewing the third party's own security practices and whether its access to sensitive information is appropriately limited.

The IRS should be vigilant about the nature of its partner, extending to organizational culture and individual employees' attitudes about security, Christian said. An online system is only as secure as its weakest link, which for a large organization is often a smaller outside partner, he said, adding that many recent breaches of major companies started with attacks on a third party.

Seeming to address that general concern, the IRS said its outside partners' role and access to taxpayer information would be minimal. "Third-party contractor involvement will be limited to taxpayer identification matching, and no taxpayer information will be permanently stored by the contractor or used for any other purposes," the IRS said. It emphasized that it would "continue monitoring the protection of taxpayer data" throughout its systems and processes.

The e-authentication process's success will ultimately depend on the third party's ability to implement the IRS's vision for the partnership, Christian said.

That inherent lack of direct control could be a major source of risk, but the IRS said it "has aggressively conducted contractor security assessments to confirm that all systems are secure."

New Mobile Threats

The IRS has faced recent scrutiny over its use of single-factor, knowledge-based authentication to secure its online applications, such as electronic filing and identity protection personal identification numbers. (Prior coverage: *Tax Notes*, Mar. 14, 2016, p. 1250; and *Tax Notes*, Feb. 29, 2016, p. 975.)

> ***There is a new class of cybersecurity threat designed to bridge that gap and target mobile devices, Ensey said.***

The e-authentication process described in the IRS slide show would be multifactor, with the two factors being the filer's knowledge of personally identifiable information and her possession of a mobile phone or email account to receive a verification code, Ensey said.

Ensey explained that text messaging a verification code to a mobile phone is known as "out of band" authentication because the confirmation occurs through a channel separate from that of the original user session — a taxpayer accessing IRS.gov — with separate servers.

However, there is a new class of cybersecurity threat designed to bridge that gap and target mobile devices, exemplified by the so-called Zeus family of malware, Ensey said. One of these programs, "Zeus-in-the-Mobile" (or ZitMo), has been used to defeat text-message-based, two-factor authentication used by banks, he said.

Ensey said some versions of Zeus are smart enough to attack a user's desktop computer first, actually initiating a text message to then compromise the user's mobile device, so it can intercept out-of-band confirmation codes tied to a desktop Web browsing session. "The same style of attack could be customized for the IRS website," he said. ■

band'' authentication because the confirmation occurs through a channel separate from that of the original user session — a taxpayer accessing IRS.gov — with separate servers.

However, there is a new class of cybersecurity threat designed to bridge that gap and target mobile devices, exemplified by the so-called Zeus family of malware, Ensey said. One of these programs, ''Zeus-in-the-Mobile'' (or ZitMo), has been used to defeat text-message-based, two-factor authentication used by banks, he said.

Ensey said some versions of Zeus are smart enough to attack a user's desktop computer first, actually initiating a text message to then compromise the user's mobile device, so it can intercept out-of-band confirmation codes tied to a desktop Web browsing session. ''The same style of attack could be customized for the IRS website,'' he said. ■

As Staff Levels Fall, IRS Bonds Team Streamlines

By Fred Stokeld — fred.stokeld@taxanalysts.org

The IRS Office of Tax-Exempt Bonds (TEB), faced with fewer employees, is taking steps to make its operations more efficient, including in the area of voluntary compliance, according to the head of the office.

TEB Director Rebecca Harrigal reported March 10 that last year TEB lost seven people and expects to lose more this year. That will probably leave TEB's staffing level in the low 60s, she said in an appearance at a National Association of Bond Lawyers program in Washington.

''Now from a big picture, when you look at the amount of bonds that are out there in ratio to the number of people in TEB, what's the big deal?'' Harrigal asked. ''But when you start looking at the work we do in TEB, it is a big deal.''

Harrigal acknowledged that the staff reduction has resulted in fewer examinations, remarking that with fewer employees, ''we're going to do less work.'' However, she cautioned against reading too much into pure numbers.

Throughout the session, Harrigal emphasized that TEB is dealing with the staff cutbacks by streamlining and standardizing operations and trying to make its processes more efficient. The office is looking at what can be cut and how it can ''help issuers do self-monitoring, self-enforcement, come in on their own when there's a problem,'' she explained.

> ***'We test effectiveness as to how early you caught the problem. The earlier you caught it, the better deal you get,' Harrigal said.***

One way TEB is streamlining its voluntary closing agreement program (VCAP) is by allowing bond issuers whose situations meet VCAP requirements to complete and sign closing agreements, compute the resolution amounts, and mail the agreements to the IRS. The option was first made available to issuers of qualified section 501(c)(3) bonds.

The simplified VCAP ''tells exactly what the settlement amount should be and what [the issuers] need to pay,'' Harrigal said. ''The issuer just fills in the blank, pays the amount, signs three copies, sends it in. We make sure everything's OK, we sign it, send it back, the case is done. There is no more