MULTINATIONAL

Tax Agency Telework Increases Fraud and Confidentiality Risks

by William Hoke

With many tax administrators working at home and accessing department systems online, agencies' long-standing challenges of maintaining taxpayer confidentiality and preventing fraud — especially involving pandemic stimulus programs — have been exacerbated, observers say.

Tax agencies contacted by *Tax Notes* say they are aware of the issues, have taken precautions, and are carrying out their missions safely and securely, but not everyone agrees.

Kimberly Houser, a professor at Oklahoma State University's school of business, said it is impossible for tax agencies to maintain the same level of taxpayer confidentiality as when their employees are working in the office.

Houser, who has written extensively on data privacy issues, said the increased level of tax agency work being done remotely is likely to result in a higher number of successful requests for bogus refunds based on identity theft or other fraudulent schemes. "If a home computer is being used to access a server at work, this creates an entry for a bad actor to gain access to the data on that server," Houser said. "The main way bad actors gain access is through phishing, ransomware, and viruses — all of which are emphasized when using a home computer. In addition, security software is not automatically updated on home computers as it is on most work computers, leaving gaping holes."

Paolo Balboni, a professor at Maastricht University in the Netherlands who specializes in privacy, cybersecurity, and IT contract law, said European tax agencies should already have solid policies, procedures, and processes in place to manage their normal workflows, even when staff are telecommuting. "It is important to make sure that employees know how to correctly handle information remotely, respecting security procedures and preserving confidentiality at all times [while] also possibly being able to recognize fraudulent communications in terms of phishing and other types of cyberattacks," he said. "Any

last-minute adjustment in terms of the acquisition of new technologies to enable work processes and organizational procedures may result in jeopardizing the security and privacy of taxpayer information."

Balboni said the number of cyberattacks and online scams started increasing after COVID-19 was declared a pandemic. "Tax agencies will surely not be spared by criminals," he said. "They need to raise the attention of their employees in order to comply with security procedures and try to recognize possible fraudulent patterns."

On April 8 the U.K. National Cyber Security Centre (NCSC) and the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued a joint advisory about what they described as an increasing number of malicious cyber actors exploiting the COVID-19 pandemic. "In the U.K., the NCSC has detected more U.K.-government-branded scams relating to COVID-19 than any other subject," the advisory says. "At the same time, the surge in home working has increased the use of potentially vulnerable services, such as virtual private networks (VPNs), amplifying the threat to individuals and organizations."

One area of concern highlighted in the advisory involves text messages. "Historically, [short message service (SMS)] phishing has often used financial incentives, including government payments and rebates, such as a tax rebate, as part of the lure," the NCSC and CISA said. "Coronavirus-related phishing continues this financial theme, particularly in light of the economic impact of the epidemic and governments' employment and financial support packages. It is likely that they will use new government compensation schemes responding to COVID-19 as themes in phishing campaigns."

On April 8 the Treasury Committee of the House of Commons held a virtual hearing on HM Revenue & Customs' handling of the economic impact of the pandemic, with a focus on whether the agency's resources and systems can cope with increased claims under new relief schemes like the coronavirus job retention scheme and the self-employment income support scheme. HMRC Chief Executive Jim Harra told the committee his agency "had to set up schemes very rapidly, and time has been the enemy of perfection" in designing and implementing them.

An HMRC spokesman told *Tax Notes* that fraudsters are indeed taking advantage of government support measures for people and businesses affected by the pandemic. "Scammers text, email, or phone taxpayers, offering spurious financial support or tax refunds, sometimes threatening them with arrest if they don't immediately pay fictitious tax owed," he said in an email. "These scams often target the elderly and vulnerable. Several of the scams mimic government messages, such as, 'Stay at home; protect the [National Health Service]; Save lives,' as a way of appearing authentic and unthreatening."

The spokesman said HMRC has a dedicated customer protection team in its cybersecurity operations working continuously to identify fraudsters.

While Harra admitted that HMRC has been "profoundly affected" by COVID-19, he cautioned against expecting the agency to do the impossible. "I think this experience has shown that HMRC can do things we didn't think we could do," he said, "but I fear that, after this, ministers will expect HMRC to do everything in one month."

In India, the Income Tax Department advised taxpayers April 8 to guard against possible breaches of their e-file accounts. The agency said it issued the warning "in the wake of an increased vulnerability and attacks on online systems as the country and the world battle the COVID-19 pandemic and more online systems are being used due to a major scaling down of human interface."

Strained Systems

The potential duration and severity of the pandemic present unique challenges for tax administrations, said the OECD Forum on Tax Administration (FTA) April 7. "The nature of the COVID-19 pandemic is placing great strains on how tax administrations can carry out their core functions efficiently and safely," FTA Chair Hans Christian Holte said.

The FTA collaborated with the Intra-European Organization of Tax Administrations and the Inter-American Center of Tax Administrations on an April 7 document outlining business continuity considerations for tax agencies

formulating their responses to COVID-19. "During a pandemic . . . it becomes more likely that critical vulnerabilities may materialize more widely than, for example, in a one-off event, and this may impact mitigation actions, which may assume a degree of independence of vulnerabilities," the document says. "Tax administrations may . . . wish to put in place specific measures to detect fraudulent schemes set up to take advantage of circumstances that greatly impact the work arrangements of the administration. This could include new schemes to obtain refunds, access government payments meant to assist taxpayers in emergencies, etc."

While tax agencies need to remain vigilant, the COVID-19 pandemic is curtailing their audit activities. The *Financial Times* reported April 14 that HMRC has advised many taxpayers under audit that it will not request information or push for responses, with some audits being suspended completely, because of the constraints imposed on the agency.

In the United States, the IRS said March 25 that while all in-person meetings for audits would be suspended, the agency's staff would continue examinations remotely, when possible. Similarly, the IRS said it had suspended all lien and levy activities, including seizures of personal residences, through July 15. "However, field revenue officers will continue to pursue high-income nonfilers and perform other similar activities where warranted," it said.

On April 9 Deputy National Taxpayer Advocate Bridget Roberts said the IRS had been procuring "tens of thousands" of laptop computers configured to allow its employees to telework.

The potential for problems with the U.S. government's rush to pump billions of dollars into the hands of Americans affected by the pandemic was illustrated late Friday, April 10, when a northwest Indiana man checked his bank balance at an ATM and saw a deposit for $8.2 million instead of the $1,700 stimulus check he had been expecting. When Charles Calvin, a volunteer firefighter, called his bank the following Monday, the erroneous deposit was no longer there. Calvin told the *Chicago Tribune* that while it wasn't clear whether the error was caused by the federal government, the bank, or the particular ATM he had used, he was just happy to end up with the amount to which he was entitled. "You go from being a millionaire one second then back to being broke again," he said. "But hey, once you're poor you don't have anywhere else to go but up."

The Dutch Tax Administration (DTA) said approximately two-thirds of its 30,000 employees are working remotely. "People with vital jobs can go to [the office], where there are other measures, such as that [staff] should be more than 1.5 meters apart," said Erik Jeene, a spokesman for the agency.

Jeene said the agency's taxpayer confidentiality standards are applicable wherever its staff are working. "IT infrastructure is secured," he said. "It does not matter whether one works from home or from the office. There are rules for this — for example, regarding whether or not one can take a physical file home; this is limited."

Jeene said he is not aware of any recent increase in fraudulent refund claims. "More than 99 percent of Dutch residents do their taxes via internet and the special program developed by the DTA, in which the DTA already fills in many facts, such as bank accounts, income, etc., that you then have to check and/or correct," he said in an email. "You can only log in with your own personal login and often [there is] extra verification through SMS. And when changing your bank account, you usually get a confirmation on paper."

The HMRC spokesman said more than 80 percent of the agency's staff are working remotely. "Our civil servants are used to work[ing] with the utmost discretion and handling sensitive information," the spokesman said. "Working from home doesn't change this professionalism."

The Canada Revenue Agency has strict security measures in place to ensure the safety of taxpayer information, agency spokesman Alex Igolkine said. The CRA said many staff members working offsite can connect remotely to the agency's systems using a fully secure virtual private network.

Whether CRA employees are working in the office or at home, they must continue to safeguard protected information, Igolkine said. "For example, paper documents containing sensitive information must be safeguarded, and approved

equipment must be used, such as CRA computers and portable data storage devices with appropriate safeguards to perform work from home," he said.

Working outside the office has been long-standing practice for many CRA employees, especially the agency's tax auditors. "As a result, the CRA has well-developed policies and controls that employees must follow in order to protect sensitive information when outside of the office," Igolkine said. "The CRA security procedures generally address various different working scenarios, including teleworking, and, as a result, our employees are trained and have access to procedures that must be followed for protecting information regardless of the location from which they work."

The pandemic has led the CRA to adopt procedures that normally would not be permitted in order to provide taxpayers with timely assistance. "For example, [we have authorized] the use of cellular phones by employees answering phone calls of Canadians in the interest of enabling the CRA to answer as many calls as possible," Igolkine said.

Before revising its procedures, the CRA carries out an evaluation to understand the potential risks and identify additional controls or mitigation efforts that can be undertaken to minimize possible problems. "Once this evaluation is completed and an informed risk decision is taken, instructions and procedures are distributed to employees on the additional steps that need to be taken — for example, informing the taxpayer that the phone call is being taken from a cell phone and providing the caller an opportunity to pursue other means of communicating with the CRA," Igolkine said.

Zoombombing

Both the DTA and HMRC said they use video conferences for staff meetings. The CRA said all of its teleconferences are conducted over the government's system. "While video conferencing is also available, [it is] currently discouraged, unless necessary, in order to minimize the burden on the CRA's IT network," Igolkine said.

The corporate world's widespread switch to teleconferencing over platforms provided by Zoom Video Communications and Microsoft have led to "zoombombing," a practice in which unauthorized individuals gain access to a video meeting and disrupt the session. A more serious concern to tax agencies would be an undetected intrusion to a teleconference during which agency employees are discussing confidential taxpayer information. "This is just one of the many ways hackers can gain access to [confidential] information," Houser said. "The IRS has a poor track record to begin with when it comes to protecting our data."

The NCSC and CISA advisory says malicious cyber actors have been sending phishing emails to exploit the increasing use of Zoom and Microsoft Teams platforms. "In addition, attackers have been able to hijack teleconference and online classrooms that have been set up without security controls (e.g. passwords) or with unpatched versions of the communications platform software," the advisory says.

Balboni said zoombombing should not be tax agencies' only concern. "Zoom is not the only platform which has shown data security and confidentiality vulnerabilities and privacy compliance weaknesses," he said. "So it is paramount before selecting a product or service that any organization, including tax agencies, run the most appropriate due diligence assessments in order to provide for the maximum protection of employees and taxpayers, along with a high level of legal compliance."

Balboni said the shift to more telework by tax agency employees will cost money. "Adapting to the current situation and remote working may result in government agencies paying more than what was originally budgeted for this year," he said. On the bright side, "additional technology to enable employees to work from home; additional security to preserve confidentiality, integrity, and the remote availability of information; [and] additional training to recognize possible fraudulent patterns and on how to be more effective when working from home may eventually result in more productivity and better services to citizens," Balboni said. ■