The Contemporary Tax Journal

Volume 11
Issue 1 *The Contemporary Tax Journal Volume 11, No. 1 – Winter 2022*

Article 3

2-2-2022

Countering Identity Theft and Strengthening Data Security Practices Across the Tax Preparer Community

Patrick Ryle JD, LLM, CPA
Dalton State College, pryle@daltonstate.edu

Assyad Al-wreikat PhD
Frostburg State University, aalwreikat@frostburg.edu

Ellen Bartley CMA
Farmingdale State College, ellen.bartley@farmingdale.edu

Mark A. McKnight PhD, CFE
University of Southern Indiana, mamcknight@usi.edu

Brett L. Bueltel JD, CPA
University of Southern Indiana, blbueltel@usi.edu

Countering Identity Theft and Strengthening Data Security Practices Across the Tax Preparer Community

Patrick Ryle, JD, LLM, CPA
Assistant Professor
Wright School of Business
Dalton State College
650 College Dr.
Dalton, GA 30720
(706) 272-4572
pryle@daltonstate.edu

Assyad Al-wreikat, PhD
Assistant Professor
Frostburg State University
101 Braddock Road
Frostburg, MD 21532
(301) 687-4063
aalwreikat@frostburg.edu

Ellen Bartley, PhD, CMA
Assistant Professor
School of Business
Farmingdale State College
2350 Broadhollow Road
Farmingdale, NY 11735
(631) 553-9406
ellen.bartley@farmingdale.edu

Mark A. McKnight, PhD, CFE
Associate Professor
Romain College of Business
University of Southern Indiana
8600 University Boulevard
Evansville, IN 47712
(812) 465-1012)
mamcknight@usi.edu

Brett L. Bueltel, JD, CPA
Assistant Professor
Romain College of Business
University of Southern Indiana
8600 University Boulevard
Evansville, IN 47712
(812) 228-5172
blbueltel@usi.edu

Countering Identity Theft and Strengthening Data Security Practices Across the Tax Preparer Community

Abstract

The IRS has renewed its commitment to tackle the ongoing problem of taxpayer identity theft, announcing the 2021 "Boost Security Immunity" initiative to raise awareness among tax practitioners and strengthen data security industry wide. Considering these developments, we reexamine the 2019 Taxpayer First Act against the backdrop of a growing trend of taxpayer fraud, tax preparer duties with respect to client data, and emerging IRS and Congressional efforts to confront tax return security challenges. Holding client data remains a solemn responsibility for accountants and tax preparers. Strong security practices critical to client safety, and essential to the integrity of the federal, state, and local tax systems. The COVID-19 pandemic, and the wholesale switch to remote work conditions, further illustrates the need for a renewed commitment to vigorous data protection practices. Finally, we address the need for financial institutions to reassess and strengthen data management and security practices.

Keywords: Taxpayer First Act; Data Privacy; Data Security; Cyber Security

https://scholarworks.sjsu.edu/sjsumstjournal/vol11/iss1/3
DOI: 10.31979/2381-3679.2022.110103

Introduction

Holding client data has never been a more serious or consequential matter for accountants and tax preparers (Ryle et. al, 2020). The COVID-19 pandemic, which forced many employees to work remotely and electronically, saw significant increases in the number of identity theft originating from tax-preparers (IRS, 2021b). These events have highlighted the pressing need for a renewed commitment to ensure that tax professionals properly store and protect data. Not only must accountants protect data from exfiltration but must also comply with increasingly complex and restrictive data privacy laws (Ryle, et. al, 2021). Tax preparers have long faced the relentless attack of cybercriminals seeking to appropriate and profit from taxpayer data, and for many years, taxpayer data theft and tax return fraud cases were on the rise. Fortunately, the Internal Revenue Service (IRS) has taken firm action to address these challenges by forming the Security Summit, devoted to addressing the problem. Congress has also stepped forward to help strengthen taxpayer security by passing the 2019 Taxpayer First Act (the TFA). This paper examines the history of taxpayer fraud, emerging accountant and tax preparer data protection obligations, and the status of IRS and Congressional efforts to confront security challenges.

Taxpayer data security is essential to the integrity of the federal, state, and local tax systems. Taxpayer data has become increasingly valuable to cybercriminals bent on committing tax return and other financial fraud. While criminals have largely targeted taxpayers in the past, they have increasingly begun to focus on the preparer community, due largely to the massive amounts of personal data held by such professionals (Schlesinger and Day, 2018; Morgan, 2016; Smith, 2015). The development of the tax fraud threat into a full-scale crisis has amplified the seriousness of holding and protecting client information (Burt, 2019). To address the crisis, the IRS has now operated an industry-wide working group known as the "Security Summit" to collectively confront these challenges. Between 2015 and 2016, the IRS convened a group of state tax agencies and officials from the private-sector tax industry to create the Security Summit. The Security Summit has a total membership that includes over 40 state agencies and over 20 individuals from the private sector and organizes its work into six distinct work groups – authentication, financial services, information sharing, strategic threat assessment, communication and taxpayer awareness, and tax professional (IRS, 2019d).

Methods

We used a process of legal research and analysis to wholistically address the legal and practical issues surrounding identity theft in the tax preparation business environment. Legal research was conducted regarding data security and other legal considerations. Relevant case law, statutes, and regulations were examined as well as tax and reporting requirements to capture a wholistic view of the issues.

Once all relevant authority was researched and examined, the IRAC method of legal analysis was applied to the issues surrounding tax data security. The IRAC process includes the issue, rule, application and conclusion approach to legal research and analysis. It has been referred to

as the "most used method to express legal analysis" (Mitra, 2019).
In this analysis, the issues regarding tax data security were segregated into tax issues, privacy issues, data security issues and practical concerns. Secondly, applicable laws, rules, statutes, and financial reporting requirements were applied to present a complete understanding of the implications and applications of those rules, based on data security issues and their relevance to tax preparation. Lastly, practical guidance and advice was given based on our conclusions from our analysis.

Tax Preparer Data Security and Privacy Challenges

In 2015, the IRS received 677,000 victim reports of identity theft of tax return information (IRS 2019a). As a result, traditional challenges to data security have remained a serious and growing concern to taxpayers and accountants. CPAs and tax preparers have long held a legal obligation to maintain standards for privacy and data management to safeguard information provided by a taxpayer while preparing a return. The Financial Services Modernization Act of 1999 – known more commonly as the Gramm-Leach-Bliley Act (P.L. 106-102) – established requirements for financial institutions, including CPAs and tax preparers, concerning the collection, disclosure, and protection of consumers' nonpublic and/or personally identifiable information. Financial institutions are required to comply with the GLBA, having an
affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information and must establish and maintain a privacy policy to protect users against foreseeable security and data threats.[1]

There are three major provisions of the GLBA that govern the collection, disclosure, and protection of consumers' nonpublic personal information, or personally identifiable information: (1) the Financial Privacy Rule, (2) the Safeguards Rule, and (3) the Pretexting Protection. First, the Financial Privacy Rule[2] requires financial institutions to provide each consumer with a privacy notice explaining information collection practices. This rule further governs disclosure about why information is stored and used, how and with whom collected information is shared, and steps taken to protect and safeguard the information. Secondly, the Safeguards Rule requires that all financial institutions "develop, implement, and maintain a comprehensive information security program."[3] The third major privacy contribution of the GLBA, the Pretexting Protection, prohibits the practice of obtaining information by false pretenses, such as using phishing schemes.[4]

Accordingly, the GLBA's three major rules, financial privacy, institutional safeguards, and pretexting protection, have provided the background for privacy practices and compliance obligations for many years in the United States. In general, tax, accounting, and CPA firms,

[1] U.S.C. §6801(a).
[2] Codified at Section 15 U.S.C. §6801 et.seq.
[3] Codified at Section 15 U.S.C. §6801(b) and §6805.
[4] Codified at Section 15 U.S.C. §6821.

https://scholarworks.sjsu.edu/sjsumstjournal/vol11/iss1/3
DOI: 10.31979/2381-3679.2022.110103

regardless of size, must comply with The Gramm-Leach-Bliley Act subject to certain disclosure exemptions.[5]

IRS Takes Action to Address the Problem

The world has changed considerably since the passage of the Gramm-Leach-Bliley Act in 1999. Increased use of technology has resulted in expanded numbers of data security breaches and taxpayer identification fraud. In 2015, the IRS decided to act by devising a tax industry-wide crackdown on identity theft (McCoy, 2017). Concluding that the IRS could not solve this problem alone, then IRS Commissioner John Koskinen convened a group of tax industry stakeholders which has come to be known as the "Security Summit," to collectively tackle problems and explore solutions (IRS, 2021a). As of 2021, total membership of the Security Summit included 42 state agencies and 20 industry offices, in addition to the Internal Revenue Service. Stakeholders include tax preparers, software developers, payroll and tax financial product processors, tax professional organizations and financial institutions.

One of the Summit's major initiatives was to set up and establish the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC) (IRS, 2018b) for the purpose of enhancing fraud detection and prevent the processing of false refunds (Cohn, 2019). This tax practice industry group continues to work together to address challenging cyber-security problems. The Security Summit is divided into six working groups, each with a dedicated focus. These work groups are: (1) the Authentication Work Group, (2) the Financial Services Work Group, (3) the Information Sharing Work Group, (4) the Strategic Threat Assessment and Response (STAR) Work Group, (5) the Communication and Taxpayer Awareness Work Group, and (6) the Tax Professional Work Group. Each working group is tasked with addressing one of the many complex aspects of the cyber privacy issue. The working groups are co-led by representatives from the IRS, states, and industry (IRS, 2019d).

IRS Efforts Lead to Improved Security

Since the start of the 2015 Security Summit Initiative, the IRS has been making headway and the security landscape has steadily been improving. In its first two years, the IRS reported significant results: a "57% decline in confirmed identity theft returns and a 65% decline in the number of taxpayers reporting themselves as victims" (IRS, 2018a). Financial industry partners also contribute to the success of these initiatives, recovering more than $1.4 billion in fraudulent refunds between 2016-2018 (IRS, 2019a).

The Security Summit Initiative has issued an ongoing call for perpetual vigilance in combatting fraud and identity theft. In partnering with the tax community to get the message out to the public, the Security Summit Initiative has produced a checklist to guide tax professionals into practicing more securely and safely. This checklist is provided in Figure 1. On July 24, 2019, the IRS issued a news release reminding professional tax preparers of the Gramm-Leach-Bliley requirement to have a data

[5] Exemptions provided by 15 U.S.C. §6803(d).

protection security plan (IRS 2019b). Many of the elements of the checklist correspond to recommended actions as provided by IRS Publication 4557, which also asserts that the information security plan must be appropriate for the company's size and complexity, the nature of its business, and the type of customer information that is maintained (IRS, 2021c).

Figure 1. The Taxes-Security-Together Checklist

- Deploy the "Security Six" measures:
  - Activate anti-virus software.
  - Use a firewall.
  - Implement an effective multi-factor authentication (MFA) system (All tax return software will offer MFA beginning in 2022) (IRS, 2020).
  - Use backup software/services.
  - Use drive encryption.
  - Create and secure Virtual Private Networks.
- Create a data security plan:
  - Federal law requires all "professional tax preparers" to create and maintain information security plan for client data.
  - The security plan requirement is flexible enough to fit any size of tax preparation firm, from small to large.
  - Tax professionals are asked to focus on key risk areas such as employee management and training; information systems; and detecting and managing system failures.
- Educate yourself and be alert to key email scams, a frequent risk area involving:
  - Learn about spear phishing emails.
  - Beware ransomware.
- Recognize the signs of client data theft:
  - Clients receive IRS letters about suspicious tax returns in their name.
  - More tax returns filed with a practitioner's Electronic Filing Identification Number than submitted.
  - Clients receive tax transcripts they did not request.
- Create a data theft recovery plan including:
  - Contact the local IRS Stakeholder Liaison immediately.
  - Assist the IRS in protecting clients' accounts.
  - Contract with a cybersecurity expert to help prevent and stop thefts [6]

[6] IRS 2019b. Tax Security 2.0 – A "Taxes-Security-Together Checklist." IR-2019-122 (July 9, 2019). Available at:https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist.

https://scholarworks.sjsu.edu/sjsumstjournal/vol11/iss1/3
DOI: 10.31979/2381-3679.2022.110103

The 2019 The Taxpayer First Act (TFA)

On July 1, 2019, Congress joined the efforts to strengthen taxpayer data security and IRS privacy practices when the President signed into law the bi-partisan Taxpayer First Act (TFA). The TFA is designed to strengthen cybersecurity by imposing stricter security and data protection standards on tax practitioners (Kess and Hurok, 2019). Section 2001 of the TFA provides that the Treasury Department must:

(1) Work collaboratively with the public and private sectors to protect taxpayers from identity theft refund fraud,
(2) Ensure that the Electronic Tax Administration Advisory Committee studies and makes recommendations on methods to prevent identity theft and refund fraud,
(3) Establish a program to issue an identity protection identification number to taxpayers,
(4) Establish a single point of contact in the IRS for taxpayers whose returns have been adversely affected due to a tax-related identity theft,
(5) Notify taxpayers of suspected identity theft, and
(6) Develop and implement publicly available guidelines
    a. for management of cases involving identity theft
    b. refund fraud

(Taxpayer First Act, 2019, §2001).

TFA Identity Protection Personal Identification Number

Taxpayer identification challenges remain a major problem. Largely due to data breaches, the reliability of traditional identification methods such as the Social Security number have now been compromised beyond repair. To this point, a 2019 Government Accountability Office (GAO) report posited that "large-scale data breaches like the 2017 Equifax hack have made Social Security numbers and other signifiers so prevalent on the black market that they are essentially useless for authentication" (Johnson, 2019). Over the long run, the IRS and Congress have determined that the reduction in the reliability of social security numbers as a means and method of identifying taxpayers, requires the development of a new identification method.

To address the demise of the reliability of Social Security numbers, the TFA creates a new Identity Protection Personal Identification Number (IP PIN) which may eventually replace Social Security numbers as a mechanism of taxpayer identification. By 2024, the IRS must be prepared to issue IP PINs to any US resident who requests one (TFA, 2019, §2005).

The TFA Raises the Stakes: Increasing Civil and Criminal Penalties

The impact of data theft to taxpayers is frightening. While taxpayer victims of identity theft face significant financial and legal consequences, which can last a lifetime, the risks to tax preparers are

also severe. Failure to take measures to properly protect client data has traditionally exposed accountants to potential civil liability as well as possible disciplinary actions by licensing authorities and the IRS. Moreover, accountants could traditionally even face criminal liability under I.R.C. §7216 for failing to take necessary data security measures (Roane, 2016). I.R.C. § 7216 and §6713 impose serious criminal and monetary penalties on tax preparers who knowingly or recklessly disclose tax return-related client data or information. Pre-existing criminal penalties under IRC §7216 and §6713 provide serious criminal and civil penalties for return preparers who wrongfully disclose information provided in assistance with a taxpayer return.[7] Prior to the TFA, the civil penalty is $250 for each unauthorized disclosure or use, up to $10,000 per calendar year. The corresponding criminal penalty is a misdemeanor, with a fine of up to $1,000, one year of imprisonment, or both (Petronchak, 2019).

The TFA has increased the severity of civil and criminal penalties for failure to protect taxpayer data. Under new provisions of the TFA, tax preparer penalties will increase. Congress is serious about strengthening cyber security standards and has notably increased the criminal financial penalties. Specifically, under the TFA, the penalty is increased for improper use or disclosure in connection with a crime relating to the theft of a taxpayer's identity (whether or not it involves any tax filing). In these instances, the civil penalty is increased from $250 to $1,000. The calendar-year limitation is also increased, from $10,000 to $50,000. The maximum fine under a criminal penalty for a violation involving identity theft is now increased to $100,000 (Petronchak, 2019).

Recommendations for Practice

Data protection is of heightened concern as many employees were forced to work from home during the coronavirus pandemic. As many companies reimagine and reorient workspaces, work-from-home or hybrid arrangements are likely to be an ongoing part of the employment landscape. Practitioners must take data protection and privacy obligations seriously and deliberately. The stakes have never been higher, and accountants must make a commitment in time and resources to managing and protecting data. A good place to start the process would be by conducting a thorough independent third-party organizational risk assessment, as well as by appointing an organizational Chief Information Security Officer (CISO).

It is incumbent upon all financial institutions to perform an assessment of their current status with regard to data management. At a minimum, this assessment should include a mapping process of the firm's security organizational control system, and an examination of the following questions:

1. What controls are in place to protect this information and the firm/organization's data infrastructure?
2. What defenses exist and how can they be strengthened?
3. What are your firm's weaknesses and how can you reduce them?
4. Does your firm have a response and notification process in place in the event of breach?
5. Does your firm have adequate insurance coverage?

[7] 26 U.S.C. § 6713; 26 U.S.C. 7216.

https://scholarworks.sjsu.edu/sjsumstjournal/vol11/iss1/3
DOI: 10.31979/2381-3679.2022.110103

Recommendations for Further Research

The enormity of cyber-privacy issue is one that will require ongoing vigilance in the field, co-operation among many agencies at the international, national, state, and local levels, and presents many opportunities for further research. Some of the areas that we recommend for further research are: assessing compliance by financial institutions with recently enacted legislation, determining the efficacy of such compliance, and examining challenges in implementing strong cyber security protection practices. Additional research should also include analyses of data protection in the work-from-home and hybrid environments.

Conclusion

Currently, every state has some regulation defining how companies must respond to a data breach. Moreover, recently passed legislation at the state and international level, such as the California Consumer Privacy Act (CCPA), and the European General Data Protection Regulation (GDPR), currently extend liability to holders of personal information/data who are subject to a breach.

However, these measures address breaches that have already occurred. CPAs and their clients must (1) question the extent to which they need to obtain and hold consumer data, (2) assess the current processes in place, (3) implement a rigorous internal system to protect this data, and ultimately the consumers whose data the firms hold, and (4) continue to monitor current trends in data management in the ever-changing technology landscape. Possession of data carries with it serious responsibilities and major risks. Consumer privacy rights and a corresponding business responsibility to protect consumer data have become one of the leading business issues of our time. Failure to proactively manage this challenge can expose financial institutions, which include CPA and accounting firms, to substantial exposure and associated costs.

References

Barrett, C. (2019). Are the EU GDPR and the California CCPA becoming the de facto global standards for data privacy and protection? *Scitech Lawyer* (Spring) 15(3): 24-29.

Burt, A. (2019). New Laws on Data Privacy and Security Are Coming. Is Your Company Ready? *Harvard Business Review* (July 31, 2019). Available at: https://hbr.org/2019/07/new-laws-on-data-privacy-and-security-are-coming-is-your-company-ready.

California Consumer Privacy Act of 2018, California Civil Code § 1798.100-199.
Cohn, M. (2019). IRS program to prevent personal data loss is delayed. *TaxProToday* (August 26, 2019).

The CPA Journal. (2001). New FTC privacy disclosure rules. Available at: http://archives.cpajournal.com/2001/0700/nv/nv10.htm.

Federal Trade Commission v. Facebook. (2019).
The Financial Services Modernization Act of 1999, Gramm-Leach-Bliley Act (P.L. 106-102) (1999).

Internal Revenue Service. (2018a). Key IRS identity theft indicators continue dramatic decline in 2017; Security Summit marks 2017 progress against identity theft. (February 8, 2018). Available at: https://www.irs.gov/newsroom/key-irs-identity-theft-indicators-continue-dramatic-decline-in-2017-security-summit-marks-2017-progress-against-identity-theft.

Internal Revenue Service. (2018b). Identity theft tax refund fraud information sharing and analysis center annual report. Available at: https://www.irs.gov/pub/newsroom/IDTTRF%20ISAC%20April%202018%20Annual%20Report.pdf.

Internal Revenue Service. (2018c). Tips for tax preparers on how to create a data security plan. IRS Tax Tip 2018-151. (September 27, 2018). Available at: https://www.irs.gov/newsroom/tips-for-tax-preparers-on-how-to-create-a-data-security-plan.

Internal Revenue Service. (2019a). IRS, Security Summit partners mark significant progress against identity theft; key taxpayer protection trends continue. IR-2019-66, (April 8, 2019). Available at: https://www.irs.gov/newsroom/irs-security-summit-partners-mark-significant-progress-against-identity-theft-key-taxpayer-protection-trends-continue.

Internal Revenue Service. (2019b). Tax Security 2.0 – A "Taxes-Security-Together Checklist." IR-2019-122 (July 9, 2019). Available at: https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist.

https://scholarworks.sjsu.edu/sjsumstjournal/vol11/iss1/3
DOI: 10.31979/2381-3679.2022.110103

Internal Revenue Service. (2019c). IRS, states, and industry offer tips to tax professionals on spotting signs of client data theft, IR-2019-140 (August 6, 2019). Available at: https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-4.

Internal Revenue Service. (2019d). Security Summit. (August 13, 2019). Available at: https://www.irs.gov/newsroom/security-summit.

Internal Revenue Service. (2020). All tax prep software will offer multi-factor authentication beginning in 2021. Available at: https://www.irs.gov/newsroom/all-tax-prep-software-will-offer-multi-factor-authentication-beginning-in-2021.

Internal Revenue Service. (2021a). Security Summit: Protecting taxpayers from identity theft tax refund fraud. Available at: https://www.irs.gov/newsroom/security-summit.

Internal Revenue Service. (2021b). IRS Security Summit announces summer campaign to raise awareness among tax pros about identity theft; urges practitioners to boost security immunity. Available at: https://www.irs.gov/newsroom/irs-security-summit-announces-summer-campaign-to-raise-awareness-among-tax-pros-about-identity-theft-urges-practitioners-to-boost-security-immunity.

Internal Revenue Service. (2021c). Publication 455: Safeguarding taxpayer data. Available at: https://www.irs.gov/pub/irs-pdf/p4557.pdf.

Johnson, D. 2019. New law brings big change to IRS in IT, cyber. *FCW, The Business of Federal Technology* (July 02, 2019).

Karl, E. (2017). The Gramm-Leach-Bliley Act still applies to CPAs. AICPA (Nov 21, 2017). Available at: https://blog.aicpa.org/2017/11/the-gramm-leach-bliley-act-still-applies-to-cpas.html.

Kess, S. and S.I. Hurok. (2019). Top ten changes in the Taxpayer First Act of 2019. *The CPA Journal* 89: 68-69, (Aug 2019).

McCoy, K. (2017). IRS: Public-private crackdown slashes identity theft, tax refund fraud. *USA Today* (October 17, 2017). Available at: https://www.usatoday.com/story/money/2017/10/17/irs-public-private-crackdown-slashes-identity-theft-tax-refund-fraud/772302001/.

Morgan, S. (2016). IRS reports 700,000 U.S. taxpayers hacked and 47 million 'Get Transcripts' ordered. *Forbes* (Feb 28, 2016). Available at: https://www.forbes.com/sites/stevemorgan/2016/02/28/irs-reports-700000-u-s-taxpayers-hacked-and-47-million-get-transcripts-ordered/#169fe5377b93.

Petronchak, K. (2019). Taxpayer First Act Changes the Dynamic Between IRS and Practitioners. *The Tax Adviser* (October 1, 2019).

Roane, D. (2016). Keeping clients' tax data secure. *Journal of Accountancy* (October 1, 2016). Available at: https://www.journalofaccountancy.com/issues/2016/oct/how-to-secure-tax-data.html.

Romm, T. (2019). U.S. government issues stunning rebuke, historic $5 billion fine against Facebook for repeated privacy violations. *The Washington Post*. (July 24, 2019).

Ryle, P.M., Bueltel, B. L., Walker, A. K., Gabrini, C., & McKnight, M.A. (2020). *The impact of the Facebook court order & CCPA 2020: Helping businesses and accountants meet the challenge of the new era of privacy compliance.* Journal of Accounting, Ethics and Public Policy, 21(2), pp 247-262. Available online at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3615422.

Ryle, P.M., Bueltel, B. L., McKnight, M.A. & Beckman, J. (2021). *Decoding lessons from the Facebook Consent Decree: Does Sarbanes Oxley foreshadow the future of privacy regulation?* International Journal of Disclosure and Governance, https://doi.org/10.1057/s41310-021-00124-2.

Schlesinger, J. and A. Day. (2018). Cybercriminals now targeting tax pros to cash in on fraudulent returns. CNBC News (April 15, 2018). Available at: https://www.cnbc.com/2018/04/14/cybercriminals-now-targeting-tax-pros-to-cash-in-on-fraudulent-returns.html.

Smith, J.F. (2015). Cyberattack Exposes I.R.S. Tax Returns. *The New York Times* (May 26, 2015). Available at: https://www.nytimes.com/2015/05/27/business/breach-exposes-irs-tax-returns.html.

United States Government Accountability Office. (2019). Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Process. (May 2019) GAO-19-288. Available at: https://www.gao.gov/assets/gao-19-288.pdf.

https://scholarworks.sjsu.edu/sjsumstjournal/vol11/iss1/3
DOI: 10.31979/2381-3679.2022.110103