Current Federal Tax Developments

Week of May 13, 2019

Edward K. Zollars, CPA
(Licensed in Arizona)

ACCOUNTING
CONTINUING EDUCATION

KAPLAN

CURRENT FEDERAL TAX DEVELOPMENTS
WEEK OF MAY 13, 2019

Published in 2019 by Kaplan Financial Education.

Printed in the United States of America.

Current Federal Tax Developments

Kaplan Financial Education

Table of Contents

Section: Security
GAO Issues Report Recommending Stronger Oversight of IT Security for E-File Providers and Software Developers

Citation: IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices, United States Government Accountability Office, GAO-19-340, 5/9/19

The Government Accountability Office (GAO) turned out to have excellent timing, releasing its report on the overall security of components of the commercial tax preparation systems in the week when Wolters Kluwer took down its online systems used by tax preparers due to a discovery of malware in their network. The report (*IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices*, United States Government Accountability Office, GAO-19-340, May 2019) recommends generally that the IRS attempt to impose specific security rules on all participants (tax preparers, electronic return originators and software developers), but the IRS disagreed with the recommendation, primarily based on their view that they lack statutory authority to take the actions suggested.

Specifically, the GAO reported the following findings:

> *Paid Preparers. IRS has not developed minimum information security requirements for the systems used by paid preparers or Authorized e-file Providers. According to IRS's Office of Chief Counsel, IRS does not have the explicit authority to regulate security for these systems. Instead, the Internal Revenue Code gives IRS broad authority to administer and supervise the internal revenue laws. The Department of the Treasury has previously requested additional authority to regulate the competency of all paid preparers; GAO has also suggested that Congress consider granting IRS this authority. Congress has not yet provided such authority. Neither the Department of the Treasury request nor the GAO suggestion included granting IRS authority to regulate the security of paid preparers' systems. Having such authority would enable IRS to establish minimum requirements. Further, having explicit authority to establish security standards for Authorized e-file Providers' systems may help IRS better ensure the protection of taxpayers' information.*
>
> *Tax Software Providers. As part of a public-private partnership between IRS and the tax preparation industry, 15 tax software providers voluntarily adhere to a set of about 140 information security controls developed using guidance from the National Institute of Standards and Technology (NIST). However, these controls are not required, and these providers represent only about one-third of all tax software providers. Additionally, IRS established six security, privacy, and business standards for providers of software that allows individuals to prepare their own tax returns (as opposed to software that paid preparers use). However, IRS has not substantially updated these standards since 2010, and they are, at least in part, outdated. For example, IRS cites an outdated encryption standard that NIST recommends not using due to its many known weaknesses.*[1]

---

[1] *IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices*, United States Government Accountability Office, GAO-19-340, May 2019, preface- GAO Highlights (PDF pages 3-4)

The report makes the following eight recommendations to the IRS:

> *The Commissioner of Internal Revenue should develop a governance structure or other form of centralized leadership, such as a steering committee, to coordinate all aspects of IRS's efforts to protect taxpayer information while at third-party providers. (Recommendation 1)*
>
> *The Commissioner of Internal Revenue should modify the Authorized e-file Provider program's requirements to explicitly state the required elements of an information security program as provided by the FTC Safeguards Rule. (Recommendation 2)*
>
> *The Commissioner of Internal Revenue should require that all tax software providers that participate in the Authorized e-file Provider program follow the subset of NIST Special Publication 800-53 controls that were agreed upon by the Security Summit participants. (Recommendation 3)*
>
> *The Commissioner of Internal Revenue should regularly review and update the security requirements that apply to tax software providers and other Authorized e-file Providers. (Recommendation 4)*
>
> *The Commissioner of Internal Revenue should update IRS's monitoring programs for electronic return originators to include techniques to monitor basic information security and cybersecurity issues. Further, IRS should make the appropriate revisions to internal guidance, job aids, and staff training, as necessary. (Recommendation 5)*
>
> *The Commissioner of Internal Revenue should conduct a risk assessment to determine whether different monitoring approaches are appropriate for all of the provider types in the IRS's Authorized e-file Provider program. If changes are needed, IRS should make appropriate revisions to the monitoring program, internal guidance, job aids, and staff training, as necessary. (Recommendation 6)*
>
> *The Commissioner of Internal Revenue should standardize the incident reporting requirements for all types Authorized e-file Providers. (Recommendation 7)*
>
> *The Commissioner of Internal Revenue should document intake, storage, and sharing of the security incident data across IRS offices. (Recommendation 8)*[2]

As has already been noted, the IRS disagreed with most of these recommendations, primarily based on the agency's view that it lacks the authority to impose mandatory requirements on the affected third parties. In the agency's response to the draft report, the IRS only agreed with recommendations 4, 7 and 8.

While the IRS's position was that they lacked authority to impose additional conditions on e-file providers and software developers, the GAO argued that this was not the case since the IRS controls who can be part of the e-file program. As well, since this report was written and responded to before the malware incident involving Wolters Kluwer came to light, it remains to be seen if the IRS will now decide to accept the GAO's or, in the alternative, if Congress might move to give the IRS the authority the agency claims it lacks to impose such conditions.

As well, the GAO refers to FTC standards that do apply to all paid preparers and software providers, standards the GAO found many paid preparers were unaware of. The report notes:

> *The Gramm-Leach-Bliley Act provided FTC with the authority to require that financial institutions subject to its jurisdiction ensure the security and confidentiality of customer records and nonpublic*

---

[2] *Ibid, pp. 39-40*

personal information; protect against any anticipated threats or hazards to the security of such records; and protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. FTC, in turn, issued a regulation known as the "FTC Safeguards Rule."

The FTC Safeguards Rule applies to financial institutions including third-party providers that help taxpayers file tax returns, such as paid preparers and providers of software that allows individuals to prepare their own tax returns. The FTC Safeguards Rule requires those institutions to develop, implement, and maintain a comprehensive written information security program. The program must contain administrative, technical, and physical safeguards that are appropriate to the provider's size and complexity, the nature and scope of the provider's activities, and the sensitivity of any customer information at issue.[3]

The Safeguards Rule is found at 16 C.F.R. §314.3:

§ 314.3 Standards for safeguarding customer information.

(a)Information security program. You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b)Objectives. The objectives of section 501(b) of the Act, and of this part, are to:

(1) Insure the security and confidentiality of customer information;

(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and

(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

16 C.F.R. §314.4 provides the elements to be included in the system:

§ 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate an employee or employees to coordinate your information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

---

[3] *Ibid*, p. 14

> *(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and*
>
> *(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.*
>
> *(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.*
>
> *(d) Oversee service providers, by:*
>
> *(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and*
>
> *(2) Requiring your service providers by contract to implement and maintain such safeguards.*
>
> *(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.*

As the GAO reports note, these standards apply even if they were not addressed by the IRS—the Federal Trade Commission independently was given authority to issue these regulations and have them apply to those in financial service industries, which include tax preparers. As well, the GAO notes that Revenue Procedure 2007-40 requires compliance with these rules as a condition of participating in the e-file program of the IRS.

Because of this, if a CPA firm has an "incident" the firm may be asked to produce the plan the firm is required to have under the FTC Safeguards Rule. As well, if an issue arises at a service provider used by the firm (and virtually every CPA firm who has moved beyond green pads and pencils will make use of multiple such organizations even if the firm initially believes they have remained out of the cloud), the firm may be asked to demonstrate that they performed the required oversight of the provider.

Section: Security
Wolters Kluwer CCH Systems Recovering from Malware Incident, Axcess Systems Partially Restored for Users

Citation: Brian Krebs, "What's Behind the Wolters Kluwer Tax Outage?" Krebs on Security, 5/7/19

It's been a tough few days for users of Wolters Kluwer's CCH tax products, especially for those using CCH Axcess. Wolters Kluwers' systems were affected by malware, per a company release issued the day after the outage triggered by the malware began.

The problem began early on Monday as users discovered CCH's online systems were not accessible. While those using the on-site version of CCH's tax product (ProsystemFX) lost access to electronic filing and the ability to obtain additional single return licenses to run returns if the user ran out of already downloaded permissions, those on the hosted Axcess products lost access to all programs they had licensed on the platform.

As the day continued and the products still could not be accessed, users who attempted to call support to check on the situation found the company's phone system was also down. A thread started on Reddit's /r/sysadmin subreddit where a number of users began to comment and discuss the issues.

Some users, claiming to be employees of Wolters Kluwer or have gotten information from employees of the organization, posted information about being told the systems were affected by malware and that they had been told to shut down all systems immediately. Most of these posts were eventually deleted by those that posted them, but the discussion continued there with accounting firm system administrators and CCH users as no official information emerged from the company as the day wore on.

Late on that evening (10:00 pm EDT), the first information emerged from the company in a post on the Wolters Kluwer Facebook page. That post stated:

> *On May 6, 2019, Wolters Kluwer experienced network and service interruptions affecting certain Wolters Kluwer platforms and applications. Out of an abundance of caution, we proactively took offline a number of other applications as we continue to investigate any impact. This prevented us from having adequate time to provide you advance notice, and for that we sincerely apologize.*
>
> *We are working diligently around the clock to restore service as soon as possible.*
>
> *We apologize to our customers for the inconvenience and appreciate your patience. We will provide further updates as they become available.*

At 10:46 am EDT the next day a new Facebook update added a statement that "[a]t this time, there is no indication that our customers' data has been compromised," the first indication that this was not simply a hardware failure, but some incident that led the organization to make a statement about the potential compromise of data. At 5:16 pm EDT on Tuesday another Facebook post confirmed that, as had been speculated on \r\sysadmin, malware had been found on the system, although the nature of that malware was not indicated.

In addition to the note indicating that there was no indication that data was compromised, the statement added a new assurance that caught reader's attention:

> *Also, there is no reason to believe that our customers have been infected through our platforms and applications.*

That same afternoon, IT security blogger Brian Krebs posted an article on his website that revealed one additional key piece of information that helped explain why Wolters Kluwer likely felt they had to comment on potential infection of customers.[4]

> *Early in the afternoon on Friday, May, 3, I asked a friend to relay a message to his security contact at CCH, the cloud-based tax division of the global information services firm Wolters Kluwer in the Netherlands. The message was that the same file directories containing new versions of CCH's software were open and writable by any anonymous user, and that there were suspicious files in those directories indicating some user(s) abused that access.*

---

[4] Brian Krebs, "What's Behind the Wolters Kluwer Tax Outage?" Krebs on Security, May 7, 2019, https://krebsonsecurity.com/2019/05/whats-behind-the-wolters-kluwer-tax-outage/

Shortly after that report, the CCH file directory for tax software downloads was taken offline.

The blog post contains an image from the Internet Archive's Wayback Machine of the page containing the open directory cited above. In that image it's clear the directories related to the ATX software.

As Brian notes, he was contacted by users on Monday indicating that they could no longer access the site. He wrote:

> *I do not have any information on whether my report about the world-writable file server had anything to do with the outages going on now at CCH. Nor did I see any evidence that any client data was exposed on the site.*

However, Brian did note that he found files that had apparently been placed in that directory that did not appear to originate from CCH.

> *What I did see in those CCH directories were a few odd PHP and text files, including one that seemed to be promoting two different and unrelated Russian language discussion forums.*
>
> *I sent Wolters Kluwer an email asking how long the file server had been so promiscuous (allowing anyone to upload files to the server), and what the company was doing to validate the integrity of the software made available for download by CCH tax customers.*
>
> *Marisa Westcott, vice president of marketing and communications at Wolters Kluwer, told KrebsOnSecurity on Friday that she would "check with the team to see if we can get some answers to your questions."*

However, Brian reported that, as of the time he originally published his article, he had not been contacted and he also noted that attempts to call CCH were frustrated by a message indicating that they were experiencing technical difficulties.

Mid-day Wednesday users of Axcess reported they were now able to log in and most, but not all, systems were available for use. A CCH Axcess user on /r/sysadmin posted a statement he received from CCH explaining the situation, indicating that Axcess was working but with the following restrictions:

> *Our priority has been to bring the system up and get you back to work as quickly as possible. In order to do that, we have had to make a few choices, and a few functions are currently unavailable:*
>
> - *The e-filing capability is not yet available at this time. We will notify you when it is available; please hold your e-filing until then. Should you attempt to e-file in the meantime, you will receive an upload error message. For now, please save your returns within the CCH Axcess application.*
> - *The email capability is performing slower than normal. You will notice a latency when attempting to send and receive email message.*
> - *Some articles and news are not accessible via links. Currently you will not have access to links to chat or support content; links to CCH Software news, or links to Knowledge Base Articles/Reviews.*
> - *At this time, new users cannot be activated. For now, you will not have the ability to set up new users within the CCH Axcess application.*

Interestingly, while Axcess users reported getting a notice, my firm (which is a *ProsystemFX* customer) has not received any message from Wolters Kluwer as of the time this is written (7:30 pm MST on May 8). Certainly, it appears nothing has changed for us and, as I noted, Axcess customers appear solely to have now been placed in the position we have been in since Monday. For now it appears all CCH customers are waiting to see when electronic filing comes back up, with the real concern being whether the system will be available to deal with approaching May 15 deadlines.

But the fact that CCH has now been able to bring much of Axcess back online is a good sign. Hopefully it's not a coincidence that they first worked on getting Axcess customers (who had been shut entirely out of CCH programs since Monday) to the same position that the on-site *ProSystemFX* customers have been in. That would suggest the next step is to restore those items that are being used by both sets of customers.

Unfortunately, the other concerns that many customers will have will likely take longer to address. Such malware incidents are complicated to unwind and at times additional information is uncovered as those investigating the incident continue their work. At this point, though, speculation on what may or may not be the case is not likely going to be helpful. Certainly, CCH customers will want to stay updated on any future developments that may be announced by Wolters Kluwer as their investigation of the incident continues.

As well, this should serve as a warning to all CPAs that in today's world there are actors looking to install malware in systems. Presumably Wolters Kluwer had security procedures in place that were meant to prevent this sort of incident from occurring—and, clearly, they were not able to accomplish that goal. System security is only as good as its weakest link, and quite often that weak link will be an individual in the organization that is tricked into downloading an attachment or clicking a link that allows malware to be loaded onto the network.

Both network level protections that are installed by IT and training users on how outside actors will attempt to trick them into assisting them in installing malware on the network are basic requirements of IT system security. As well, management must be constantly aware that there is no such thing as an "impenetrable network" and overconfidence in the effectiveness of existing systems is likely the biggest risk to your firm's security.

Section: 62
IRS Updates Maximum Cost of Autos for Cents-Per-Mile and FAVR for 2019

Citation: Notice 2019-34, 5/8/19

The IRS has released the maximum value for employer provided vehicles for purposes of the special valuation rule found at Reg. §1.62-21(d) and (e) for 2019 in Notice 2019-34.

In Notice 2019-08 the IRS had announced that the agency planned to issue regulations that were going to greatly increase the limits for the cost of such vehicles to take into account changes made in the Tax Cuts and Jobs Act, setting the base value at $50,000 adjusted annually for inflation after 2018.

While those proposed regulations are yet to be issued, the new Notice updates the maximum cost limit for use of a Fleet Average Valuation Rule (FAVR) plan and the cents-per-mile optional valuation method for 2019.

The notice provides:

- The maximum value of an employer-provided vehicle (including cars, vans and trucks) first made available to employees for personal use in calendar year 2019 for which the vehicle cents-per-mile valuation rule provided under Treas. Reg. § 1.61-21(e) may be applicable is $50,400.
- The maximum value of an employer-provided automobile (including vans and trucks) first made available to employees for personal use in calendar year 2019 for which the fleet-average valuation rule provided under Treas. Reg. § 1.61-21(d)(5)(v) may be applicable is $50,400.

The notice also provides relief for vehicles that were first provided to employees in years prior to 2018 that did not qualify under the then significantly lower maximum amounts. The Notice states:

> *…the Treasury Department and the IRS intend to revise Treas. Reg. § 1.61-21(e) to provide that if an employer did not qualify under Treas. Reg. § 1.61-21(e)(5) to adopt the vehicle cents-per-mile valuation rule on the first day on which a vehicle was used by an employee of the employer for personal use because, under the rules in effect before 2018, the vehicle had a fair market value in excess of the maximum permitted in accordance with Treas. Reg. § 1.61-21(e)(1)(iii), the employer may first adopt the vehicle cents-per-mile valuation rule for the 2018 or 2019 taxable year based on the maximum fair market value of a vehicle for purposes of the vehicle cents-per-mile valuation rule set forth in Notice 2019-08 or this Notice 2019-34, as applicable. Similarly, the IRS and Treasury Department intend that the proposed regulations will further provide that if the commuting valuation rule of Treas. Reg. § 1.61-21(f) was used when the vehicle was first used by an employee of the employer for personal use, and the employer did not qualify to switch to the vehicle cents-per-mile rule on the first day on which the commuting valuation rule was not used because, under the rules in effect before 2018, the vehicle had a fair market value in excess of the maximum permitted in accordance with Treas. Reg. § 1.61-21(e)(1)(iii), the employer may adopt the vehicle cents-per-mile valuation rule for the 2018 or 2019 taxable year based on the maximum fair market value of a vehicle for purposes of the vehicle cents-per-mile valuation rule set forth in Notice 2019-08 or this Notice 2019-34, as applicable.*

If an employer decides to take advantage of this relief, the notice goes on to describe a consistency rule going forward:

> *However, consistent with Treas. Reg. § 1.61-21(e)(5), an employer that adopts the vehicle cents-per-mile valuation rule must continue to use the rule for all subsequent years in which the vehicle qualifies for use of the rule, except that the employer may, for any year during which use of the vehicle qualifies for the commuting valuation rule of Treas. Reg. § 1.61-21(f), use the commuting valuation rule with respect to the vehicle.*

A similar relief provision is provided in the Notice for taxpayers wishing to switch to using an FAVR plan beginning in 2018 given the higher limits.

The IRS provides that taxpayers may rely on the provisions of this notice until the promised revised regulations are issued. The agency is also asking for comments on the notice, presumably to use in considering the development of the eventual revised regulations.

Section: 1371
Redemptions Taxed as Distributions Under §301 During Post-Transition Termination Period First Reduce AAA

Citation: Revenue Ruling 2019-13, 5/9/19

If a former S corporation makes a distribution to redeem shares that is treated as equivalent to a dividend and, therefore, taxed under IRC §301 during its post-transition termination period, how is that taxed? In Revenue Ruling 2019-13 the IRS answers that question which likely has not been keeping most of America awake at night awaiting an answer.

The relatively short ruling looks at whether that distribution first reduces the accumulated adjustment account (AAA) and the taxpayer's basis in the stock or, rather, is treated as first coming out of earnings and profits.

The post-termination transition period is a time frame following the termination of a corporation's S election when its distributions are treated as coming first of S corporation AAA and only after that is exhausted as coming out of earnings and profits.[5] There are three such periods defined in IRC §1377(b)(1):

> *(1) In general*
>
> *For purposes of this subchapter, the term "post-termination transition period" means—*
>
> > *(A) the period beginning on the day after the last day of the corporation's last taxable year as an S corporation and ending on the later of—*
> >
> > > *(i) the day which is 1 year after such last day, or*
> >
> > > *(ii) the due date for filing the return for such last year as an S corporation (including extensions),*
> >
> > *(B) the 120-day period beginning on the date of any determination pursuant to an audit of the taxpayer which follows the termination of the corporation's election and which adjusts a subchapter S item of income, loss, or deduction of the corporation arising during the S period (as defined in section 1368(e)(2)), and*
> >
> > *(C) the 120-day period beginning on the date of a determination that the corporation's election under section 1362(a) had terminated for a previous taxable year.*

The ruling provides the following fact pattern to be considered:

> *X is a corporation that once was a C corporation and later elected to be an S corporation under § 1362(a) of the Code. X's S election terminated under § 1362(d), such that it is now a C corporation. A, an individual, owns all 100 shares of the outstanding stock of X. X is a calendar-year taxpayer. At the time of its conversion to an S corporation, X had accumulated earnings and profits (E&P) of $600x and no current E&P. At the time of the termination of its S election, X's AAA was $800x and its accumulated E&P was still $600x. During X's post-termination transition period, X redeems 50 of A's 100 shares of X stock for $1,000x. X makes no other distributions during the*

---

[5] IRC §§1371(e), $1377(b)

post-termination transition period. Pursuant to § 302(d) of the Code, the redemption is characterized as a distribution subject to § 301. For the taxable period that includes the redemption, X has current E&P of $400x.

The ruling holds that this distribution first reduces AAA and the shareholder's basis in stock until the distribution has reached the level of the AAA ($800x). The remainder of the distribution ($200x) is taxed as a dividend under IRC §301(c)(1).

Section: 2058
Federal Estate Tax Deduction for Connecticut Estate Tax Must Be Reduced to Account for Tax Imposed on Add-Back of Connecticut Gift Taxes Paid Within Three Years of Death

Citation: Program Manager Technical Advice 2019-03, 5/8/19

The IRS addressed a special issue impacting the estate tax deduction under IRC §2058 for amounts paid for state estate, inheritance, legacy or succession taxes under Connecticut's estate tax. In Program Manager Technical Advice 2019-03 the IRS looks at the issue of whether the estate tax paid to the state of Connecticut has to be reduced proportionately to account for Connecticut gift taxes paid within three years of death that are included in the Connecticut taxable estate.

IRC §2058(a) provides:

> *(a) Allowance of deduction*
>
> *For purposes of the tax imposed by section 2001, the value of the taxable estate shall be determined by deducting from the value of the gross estate the amount of any estate, inheritance, legacy, or succession taxes actually paid to any State or the District of Columbia, in respect of any property included in the gross estate (not including any such taxes paid with respect to the estate of a person other than the decedent).*

The state of Connecticut, like the federal government, imposes both gift and estate taxes. Like the federal transfer tax regime, when the estate tax is computed for a Connecticut decedent those lifetime gifts and the taxes paid are taken into account when computing the Connecticut estate tax to assure that the marginal tax rate paid is based on lifetime transfers.

Connecticut also requires decedents to add back any state gift taxes within three years of the date of death to insure that those "close to date of death" state gift taxes do not escape the state's estate tax—that is, the donor has to live for three years to escape transfer taxes on the funds used to pay for the tax on such lifetime transfers.

The party to whom the advice was addressed posed three questions which the author answered as follows:

> ***(1) Are post-2004 Connecticut gifts included in the Connecticut estate tax base?***
> *No, post-2004 Connecticut gifts are not included in the Connecticut estate tax base; rather, they are included in the computation of the Connecticut estate tax to insure that the Connecticut taxable estate is taxed at the highest applicable marginal rate.*
>
> ***(2) In the case of Connecticut decedents dying after 2014, is the Connecticut gift tax paid on gifts made within three years of death included in the Connecticut***

> ***estate tax base?*** *Yes, for deaths after 2014, the Connecticut estate tax base includes Connecticut gift taxes paid on gifts made within three years of death.*
>
> ***(3) Should the deduction under I.R.C. § 2058(a) be reduced by the Connecticut estate tax attributable to the Connecticut gift taxes paid on gifts made within three years of death?*** *Yes, the Connecticut gift tax paid on gifts made within three years of death is not includible in the federal gross estate. The deduction for the Connecticut estate tax must be reduced by the amount of the Connecticut estate tax attributable to the Connecticut gift tax paid on gifts made within three years of death.*

The analysis justifies the adjustment for the amount of Connecticut estate tax paid attributable to adding back the gift taxes paid within three years of death as follows:

> *Connecticut gift taxes paid on gifts made within three years of death are not includible in the federal gross estate. See § 2035(b), including in the gross estate only the gift tax paid under Chapter 12 (the Federal gift tax) on gifts made within three years of death. As noted above, IRC § 2058 allows a deduction only for the state death taxes paid with respect to property included in the federal gross estate. Accordingly, in the case of decedents dying after 2014 who made taxable gifts within three years of death, the deduction for the Connecticut estate tax must be reduced by the amount of the Connecticut estate tax attributable to the Connecticut gift tax paid on those gifts.*

Section: 6672
Trust Fund Penalty Applies Even If Individual Was Acting Under Orders from SBA Receiver to Pay Other Creditors First

Citation: Myers v. United States, CA 11, Case No. 18-11403, 5/6/19

The Eleventh Circuit Court of Appeals rejected a unique twist on the "my boss ordered me not to pay the trust fund taxes" defense in the case of *Myers v. United States*, CA 11, Case No. 18-11403. In this case the party Mr. Myers claimed ordered him not to pay was an agent of the Small Business Administration (SBA) that had been appointed as a receiver of his employer.

The opinion summarizes the facts of this case as follows:

> *The two companies that Myers worked for were owned by another company ("Parent Company"), and Parent Company was licensed by the U.S. Small Business Administration (the "SBA") as a Small Business Investment Company (the "SBIC"). The SBA guarantees debentures that SBICs issue and has the power to place those SBICs into receivership.*
>
> *Here, Parent Company violated the terms of its license, so the SBA filed suit in the Southern District of New York to place Parent Company into receivership.*
>
> *See United States v. Avalon Equity Fund, L.P., No. 1:08-cv-7287 (S.D.N.Y., filed Aug. 18, 2008). Under an agreed-to Consent Order, the Southern District of New York placed Parent Company in receivership. Per the Consent Order, the Southern District of New York took "exclusive jurisdiction" of Parent Company and "all of its assets, and the Court appointed the SBA as Parent Company's receiver.*
>
> *As Parent Company's receiver, the SBA was given "all powers, authorities, rights and privileges . . . [enjoyed] by the general partners, managers, officers and directors" of Parent Company. In turn, Parent Company's actual general partners, managers, officers, and directors were dismissed. Put simply, the SBA was calling the shots for Parent Company.*

In 2009 the companies that Mr. Myers worked for failed to pay trust fund taxes. Mr. Myers was the CFO and co-president of the entities, and he had signature authority over the entities' bank accounts.

The problem arose while the receivership was in place, and Mr. Myers claimed that the SBA's agent handling the receivership told him to pay other creditors rather than first paying the trust fund taxes. Mr. Myers did agree to pay those vendors even though that meant the trust fund taxes remained unpaid.

The IRS eventually assessed the trust fund penalty under IRC §6672 against Mr. Myers. Mr. Myers agreed that, generally, the "my boss told me to do it" defense doesn't work in trust fund penalty cases. But he argued that this case was different—the party ordering Mr. Myers to not pay the U.S. government the trust taxes was an agent of the U.S. government.

The main opinion in the case contains a very terse and broad ruling against Mr. Myers' position, stating:

> *So, the narrow question before us is whether 26 U.S.C. § 6672(a) — and our case law interpreting it — applies with equal force when a government agency receiver tells a taxpayer not to pay trust fund taxes. We hold that it does. We cannot apply different substantive law simply because the receiver in this case was the SBA. Thus, Myers is liable under § 6672(a).*

Judge Jordan, in a concurring opinion, agreed with the result but did not agree with the broad holding that the same rule would apply in all cases. The judge notes:

> *Mr. Myers' contention is that a person should not be liable under § 6672(a) to a federal agency — the IRS — for trust fund penalties if a different federal agency— the SBA acting as receiver — has told him not to pay trust fund taxes. I am not sure this legal issue is clear cut, and I can imagine a situation — like the one presented in McCarty v. United States, 437 F.2d 961, 963–73 (Ct. Cl. 1971) — where the answer would not be self-evident.*

But this case is not such a case in Judge Jordan's view:

> *As I see things, Mr. Myers is essentially arguing that the IRS should be estopped from recovering trust fund penalties because he acted pursuant to the instructions of the SBA receiver. I would hold that, on this record, Mr. Myers' reliance on these instructions was not objectively reasonable. Cf. United States v. Alvarado, 808 F.3d 474, 484–85 (11th Cir. 2015) (explaining, in the criminal context, that the public authority and entrapment-by-estoppel defenses require reasonable reliance).*
>
> *When the SBA became the receiver of the parent company, it stepped into the private status of that entity, see Untied States ex rel. Petras v. Simparel, Inc., 857 F.3d 497, 503–04 (3d Cir. 2017), and had to abide by its own liquidation standard operating procedures. Those procedures, in relevant part, required the SBA receiver to make all appropriate filings with federal tax authorities as required by 28 U.S.C. §960 if reasonably possible. See id. at 504; Small Business Administration, SBIC Liquidation SOP 10 07 1 at Ch. 7 ¶ 7.b(2) (2007). In turn, § 960 provides that "[a]ny officers and agents conducting any business under authority of a United States court shall be subject to all Federal . . . taxes applicable to such business to the same extent as if it were conducted by an individual or corporation." Given this language, Mr. Myers could not have reasonably relied on the do-not-pay instructions of the SBA receiver. See Cal. State Bd. of Equalization v. Sierra Summit, Inc., 490 U.S. 844, 852 (1989) (explaining that Congress' intent in enacting § 960 was that "a business in receivership . . . should be subject to the same tax liability as the owner had he been in possession of, and operating, the enterprise.").*