Economic Security Project

MAY 2026

# The Future of Tax Filing

## Part 3: Beyond Direct File: A Vision for the Future of Tax System Access

### Chapter 10: IRS communications

Gabriel Zucker, Chris Given[1]

**Contents**



**Summary**

- The IRS has insufficient mechanisms to communicate easily with taxpayers in the 21st century, which has implications for many agency priorities. (10.1.1)
- Taxpayers would appreciate easier-to-access communications from the agency, something they have to come to expect from institutions in their lives — including

[1] This chapter is significantly informed by user research led by Allison Abbott.

via email. At present, though, they expect the IRS will only communicate with them for punitive purposes. (10.1.2)

- Recommendations:
    - The IRS must adopt an improved, user-friendly secure messaging platform, for those sensitive messages that require encrypted communication. (10.2.1)
    - The IRS should open the door to communicating with taxpayers via email (10.2.2). The agency should assess each communication on a case-by-case basis to determine how much can be disclosed via email, taking seriously the risk of taxpayers not receiving communications sent through other mediums, and abandoning the too-broad blanket rule of no federal tax information in unencrypted communications (10.2.3).
    - Building trust in IRS communications will take time, and the agency should pursue a program of intentionally building that trust, starting with simpler and lower-stakes messages (10.2.4). Communications should use plain language and a friendly tone, and should be user tested to ensure they are well crafted (10.2.5).
    - The IRS may also consider mass marketing campaigns in support of these direct communications reforms. (10.2.6)

---

Many potential items to improve access to the tax system, including many of the items discussed in later chapters, require the IRS to communicate directly with taxpayers. In simpler cases, these are taxpayers who have already filed and may be expecting a follow-up communication; in harder cases, they may be non-filers who do not expect to hear from the IRS at all. In easier cases, the communications do not reveal sensitive information about the taxpayer; in harder cases, they do.

And yet, the IRS's ability to communicate directly with taxpayers is, at present, incredibly limited, for legal, inertial, technological, and cultural reasons. A viable communications platform and program may seem like a banal reform item, but we believe that implementing it would unlock a great many other agency priorities, and as such ought to be prioritized. **A modern IRS needs to communicate with taxpayers like a modern organization; it needs to communicate with taxpayers like they are real human beings. This is a baseline competency that will rebuild trust and unlock other, more exciting reforms.**

# 10.1 Background

## 10.1.1 Status quo and analogous use cases

The bread and butter of IRS communications continues to be notices sent via snail mail. Moreover, for many years, the IRS has publicly signaled that the agency will never communicate with taxpayers via email or phone — and, indeed, anyone purporting to be the IRS via phone or email is ipso facto a scammer.

It is no longer quite true, though, that the IRS can *only* communicate via mail. In 2023, the IRS enabled secure online messaging via the IRS online account — for taxpayers who have an online account. (We believe this is currently approximately 30-40 million people.) That is, the agency can send a notice to a taxpayer, accessible when logged into a secure session, through the ID-verified account. Generally, the taxpayer will receive an email (or, in principle, a text message — although, as of writing, such SMS functionality has not yet been implemented) notification that they have a message in the online account, but they have to log in to see it. This is akin to how many online medical messaging services work, for example: you receive an email that you have test results from your recent visit, and you have to log in to view those results. The IRS is facing the same basic constraint: email is not a secure enough medium for highly sensitive federal tax information — though, as discussed below, this is not a cut-and-dry bar on any information in the body of an email. (Such sensitive tax information may, meanwhile, be sent via snail mail to a known address.)

This messaging system is also akin to the system established by the Department of Veterans Affairs — though there are some differences in user-friendliness of the implementations. Generally, as of this writing, if the IRS sends a notice via the online account, it is simply an electronic version of the same notice they also send in the mail. This can be unwieldy to view and interact with in a web browser, and still worse on a mobile phone. The relatively more advanced VA system sends messages better adapted to the digital format.

Of course, this entire messaging service has another, more important limitation: it's only for taxpayers who have an online account. The IRS does *not* send emails or text messages to taxpayers other than online account users receiving notifications. (In fact, sometimes taxpayers create an online account and discover a whole slew of important messages in it that they did not previously know about; notices were sent in the mail but arrived at the wrong physical address, and, without an extant online account, no electronic notifications were sent.)

Note, though, that's not because the IRS does not *have* taxpayers' contact information. Phone number is a required field on all returns, and email is a required field on all e-filed returns (which represent over 93% of individual returns). The IRS *has* non-mail contact information for taxpayers; it just does not currently use it.

Meanwhile, in the special case of Direct File users, the IRS did in fact communicate with taxpayers via email. Users received notifications from Direct File when returns were submitted, and when they were accepted or rejected by MeF. Users also got reminders to finish filing if they had partly-finished returns, and, in some cases, reminders to finish their state returns. The IRS contemplated reminder emails to taxpayers in 2025 who had used Direct File the previous tax year and not yet filed, but this functionality was not used until filing season 2026, when the IRS used it to promote other filing options following Direct File's demise.

### 10.1.2 Taxpayer perceptions

In our user research sessions, we asked taxpayers about IRS communications — both in the abstract and in the context of specific communications we proposed they could receive, including reminders to file, notifications that their withholding might be too low/high, or notices that someone else had claimed their child, for example. We heard several key themes.

**Receiving IRS notices is, today, a scary experience.** Taxpayers instinctively assume the communication means trouble.

- *"IRS messages always cause anxiety... whenever you receive anything and you see that in your inbox, you're like, oh, my God, I don't have time for this today."* — Participant #11
- *"Any time I see a letter or any notice from the IRS, I get like a little mini panic attack."* — Participant #13

This was the case even (and perhaps especially) when we asked taxpayers to consider what it would be like to receive a wholly positive notice, for example that the taxpayer was due a refund. Partially, this fear stems from the empirical fact that taxpayers have generally had the experience of receiving an IRS communication only when there is trouble. **When we showed taxpayers sample hypothetical helpful messages, they said they couldn't believe the IRS would send something like this**:

- *"Yeah, I mean, it sounds nice. I can't imagine them actually sending something that sounded like that." — Participant #13*

In the case of such non-punitive communications, **research participants suggested finding prominent ways to indicate, without having to open the (proverbial) envelope or delve deep into the message, that it was positive and non-threatening**:

- *"If there's some way that, like, in the subject, they're saying, 'don't worry' in big capital letters... The opening sentence really makes a difference... If they can add color to it, they can make it fun because it's not a penalty... they don't have to, you know, kiss the ground I walk on, but, hold my hand a little bit and wipe my brow, because now I'm sweating."* — Participant #11
- *"Maybe they should put something like, 'you're not in trouble,' like on the envelope or something — like, oh, okay, I'm not going to shred it. There's a stamp of, like, 'this is not a bill.'"* — Participant #8

We also asked taxpayers about how they communicate with other institutions in their lives that send sensitive information. **Some taxpayers told us they were used to and comfortable using secure messaging platforms in other contexts**:

- *"I work with the VA, which is a government agency, and we use a portal, which is secure... which seems to be working great for us."* — Participant #4

- *"I communicate through bank apps, I suppose, and those are usually fine, but not always really efficient."* — Participant #6

**We asked taxpayers, in an ideal world, how they would like the IRS to communicate with them. Taxpayers were enthusiastic about receiving IRS emails, and receiving messages through an online portal — both mediums that people were familiar with.** Taxpayers were, on the other hand, more skeptical of getting text messages, which they consider spammy.

- *"I would be okay with the email because I get email from everything else, my bank and every official thing I can think of. It's like the IRS is pretty much the only place that's like, no, we're not going to email you because I get email from every other thing."* — Participant #13
- *"Yeah, I think they should, they shouldn't just send the letters, like maybe emails as well. I kind of travel full-time, like, my mail is sometimes everywhere, ... correspondence from anything serious, I would hope they send it to my email, or I go on the website, so I can check it... I don't think a lot of people are checking their mail, religiously"* — Participant #7
- *"IRS does always say we will never send you unsolicited texts.... I don't like phone calls and texts because those are so spammy, but usually emails you can verify if it comes from the official web address. ... So email would be good... It's more real time. So I like that convenience."* — Participant #15
- *"I would probably prefer email. Email from the IRS seems very interesting and, or like, email to the inbox on the main portal of the IRS would be, and then get a notification to my email."* — *Participant #14*
- *"We should all have an app where they can notify us on important updates."* — Participant #3

Regarding secure communications portals in particular, we did hear **a specific complaint about platforms that hide too much information behind log in**:

- *"I don't like the ones that say, you have a new message, go log into your portal. I don't like that because then I've got to set aside time to log in. I like to be able to skim through my emails and see that, maybe save it for later. So I prefer some detail in the email... the ones that I like, you know, from credit cards, banks, medical bills, I like where it gives me some specifics as I'm skimming through."* — Participant #15

**Taxpayers do like the idea of getting helpful, non-punitive reminder messages from the IRS:**

- *"And so everything else I have in my entire life sends me letters like this to remind me to do things that I'm supposed to do. The IRS should. They don't, but they should."* — Participant #12, specifically about the idea of a reminder to file notice after April 15
- *"I think they should remind you, like, usually if you file taxes in the past, they have your email or contact information... I think they should let you know, because maybe you*

*forgot.*" — Participant #15, specifically about the idea of a reminder to file notice after April 15

**But taxpayers also believe the IRS does not currently send non-punitive messages, or emails. For taxpayers to be confident the messages are not spam, the behavior would have to be normalized; the culture would have to be shifted.**

- *"If I just got this out of the blue, I would be like, there's no way the IRS is emailing me."* — Participant #12
- *"It doesn't sound like something the IRS would do. So I think my first initial thought would be like, oh my God, it's a scam."* — Participant #9, about a potential notice that their withholding is incorrect

**To help them be confident a message was not a scam, several taxpayers mentioned sending the message via multiple means, for example via email *and* letter.** (*"I actually think it would be good to have both because then you would feel extra sure, okay, this is the IRS."* — Participant #15.) **Others mentioned sending notices indicating that the IRS *would* in the future be sending emails.** Some also floated the idea of learning about messaging campaigns via mass-market advertising:

- "*Something that makes me not feel like it's fishy....I feel like if I saw a legitimate advertisement, I would go, oh, all right, good to know.* — Participant #1, specifically in the context of promoting Direct File
- *"Maybe if I knew that they were going to start doing something like that, if they announced it...in a TV commercial."* — Participant #13
- *"I would need to be notified in some other way, maybe an official letter from the IRS, saying we're going to start using emails — or like a TV commercial, some kind of source that I could trust."* — Participant #12

## 10.2 Recommendations

The recommendations below account for the fact that *some* IRS communications contain highly sensitive federal tax information (FTI) and need to be transmitted via secure means; but some communications are not as sensitive. Section 10.2.1 concerns the transmission of secure messages; Section 10.2.2 concerns the transmission of non-secure messages; Section 10.2.3 concerns the relationship between the two. Sections 10.2.4-6, finally, concern the overall strategy of a prospective messaging program, as the IRS implements such widespread cultural changes.

### 10.2.1 Adopt an improved secure messaging platform

To transmit messages with highly sensitive FTI, a secure messaging service along the lines of the one the IRS has must remain an integral part of the system.

**One compelling possibility is that secure messaging could be a common government-wide function, built and maintained by the General Services Administration**

**(GSA). Many agencies face a broadly similar problem, with the need to securely communicate sensitive data to beneficiaries and citizens.** Each agency solving this piecemeal creates inherent inefficiencies. A prospective government-wide messaging service, in many ways conceptually analogous to GSA's Login.gov, would obviate the need for the IRS to improve its existing service. Moreover, by unifying messaging services across agencies it might promote a better experience for users who would not have to manage so many distinct government accounts; and it could promote adoption, since a user who created, say, a VA messaging account, would now immediately have an IRS messaging account, too.

**Barring a government-wide service along these lines, the IRS should simply work on improvements to the agency's existing secure messaging service.**

In either case, like the VA implementation discussed in Section 10.1.1, the messaging platform should feature as much as possible native in-app messaging rather than un-skimmable and unwieldy links to PDFs. Notifications sent by email about the existence of a new secure message need to be as detailed as they can reasonably be without compromising privacy; as taxpayers noted, bland notifications that "you have a message" are hard to work with (more on this latter point in Section 10.2.3).

### 10.2.2 Communicate with taxpayers via email

**We believe it is time for the IRS to end its (near-)blanket policy of not emailing taxpayers, and begin communicating with taxpayers via email, even outside the context of the online account.** The IRS has email addresses for the overwhelming majority of taxpayers (as they are required on all e-filed returns, which make up over 93% of returns), and can greatly improve tax administration by using them — for reminders to file, for proactive alerts, for notifications of corrections to returns, etc.

The policy of not emailing may make for a neat soundbite in anti-fraud measures. But it is simply outdated, and it comes at too great a cost. Banks and medical institutions, dealing with similarly sensitive data and communications, have not chosen to categorically eschew emailing. Moreover, as noted above, the categorical claim that the IRS will never email you is not quite true: via online account notices and Direct File communications, the IRS already does email many taxpayers. In this sense, expanding an email communication program isn't even an unprecedented crossing of the Rubicon; it is the natural outgrowth of an expansion in the use of digital platforms.

The IRS should also consider this question in light of broader taxpayer perceptions of the agency. Despite improvements after the Inflation Reduction Act, the IRS has for years battled the perception that it is unreachable, that there is no way to be in touch with the agency. More frequent email communications would help in unwinding this perception.

Anti-fraud measures will be critical as the IRS expands email communications, and a team in charge of such communications will need to carefully track the issue and respond to it dynamically over time. Some mitigation measures could include:

- Sending the same message via multiple mediums (i.e., mail, and online account secure message), so the taxpayer can confirm its veracity.
- Containing a prominent link to the secure messaging platform, where the taxpayer can confirm the message.
- IRS.gov web pages where taxpayers can confirm the veracity of the communication.
- An IRS phone number taxpayers can call to confirm the communication.
- Distinctive and consistent messages, sent from a recognizable irs.gov email address, and with clear markers in the header of the message explaining how a taxpayer can be confident this is a valid message, and how to report issues if they see a message they are skeptical of.

Of course, even with the IRS's limited emails today (principally, that is, online account notification messages), it is already possible for bad actors to attempt phishing attacks by replicating the format. Rather if IRS communications were a more routine occurrence, taxpayers would have an increased ability to recognize the format and safeguards of legitimate messages, inoculating them against scams.

Arguing that the IRS should send emails is not a claim that fraudulent messages are not an issue — but rather that fraud and risk must be appropriately contextualized and managed, and that abstinence, while it may feel like the safest option, maximizes neither security nor benefit for taxpayers.

### 10.2.3 Assess what information can be emailed on a case-by-case basis, weighing privacy against other priorities

We noted above that IRS messages may contain highly sensitive data, which it would be inappropriate and risky to put in an unencrypted email. The IRS recognizes this point with its **de facto policy that FTI cannot be put in any unencrypted message, including email. We believe that this is too strong of a rule, and that communications should instead be reviewed case-by-case, weighing the risks to taxpayer privacy against other considerations.**

First, we should note that the de facto ban on unencrypted communication of FTI is *not* statutory. Whether a given piece of data is considered FTI is effectively defined in statute. But there is no statute or regulation we know of that specifies FTI can never be included in an unencrypted email; this is just an administrative norm within the agency.

Primarily, the rule is too strong because **not all FTI is created equal.** A taxpayer's W-2, containing their Social Security Number, their precise income, and their withholding, is quite sensitive; it is hard to picture taking meaningful privacy risks with an entire W-2. The fact that a taxpayer attempted to file a return (known at the IRS as fact-of-filing), on the

other hand, is considered FTI, but it is far less sensitive, and perhaps barely sensitive at all. Indeed, fact-of-filing information is nearly-universally found in unencrypted emails sent by the tax prep industry; the data appears in tens of millions emails every year, and this has not given rise to any known identity theft vulnerabilities. It is a gross simplification to treat FTI as a monolith.

Instead, the IRS should analyze communications on a case-by-case basis — taking **a balanced view of the risks. Government agencies often tend to take a one-sided view: more disclosure increases the risk of privacy compromise, and is therefore inadvisable. But there are risks too from having a communication system that is too hard to access.** Suppose the IRS needs to communicate that a taxpayer is owed a very large refund, or that their return has an issue and needs to be resubmitted to avoid penalties, or that the taxpayer owes a debt accruing interest each day. If complex messaging systems prevent the taxpayer from seeing these messages and claiming the funds, there are real harms, which need to be weighed against the privacy risks. To put a finer point on it, suppose the IRS has evidence a taxpayer is currently the victim of identity theft, and wants to advise the taxpayer to take concrete actions to ensure the integrity of their return. In this case, if the taxpayer does not receive the message and does not take action, there could be *increased* risk of fraud and compromised privacy; in the interest of protecting privacy, in other words, the IRS would have in fact *increased* the risk of compromising it. Or, finally, suppose a blanket ban on unencrypted FTI pushes large volumes of sensitive messages into snail mail, which has been approved for sensitive data. This does not necessarily make taxpayer data any safer; mail can be compromised, too.

To its credit, in practice, the IRS sometimes recognizes all of these points. In 2024 and 2025, Direct File was permitted to send email notifications to its users about whether their returns were accepted or rejected, and reminders to file if they had not done so — emails that clearly imply fact-of-filing, and thus nominally contain FTI. The IRS made the (correct) call that, given the paramount importance of these messages, and given the low privacy risks of fact-of-filing in particular, the messages should be sent. However, these risk-based assessments are few and far between.

**Our view is that IRS communications ought to make these kinds of reviews on a case-by-case basis, rather than treating "FTI can never be emailed" as a categorical rule.** The assessment should weigh the privacy risk to the taxpayer against the value to the taxpayer and come to sensible risk-based conclusions. A message, for example, that tells a taxpayer that they didn't file for a given year and may be due a significant refund, should be able to be emailed. The communications apparatus needs an empowered team, able to make risk assessments on behalf of the agency, that can review draft communications with an eye toward finding ways to include as much information as needed to motivate action in email messages, rather than relying solely on "you have a message" notifications. Even in cases where most of a communication is protected — for example, a specific numerical update to a protected number on a tax return — unencrypted email communications can *describe the nature of this update*, while leaving the full details to a secure communications

platform. The unencrypted communication, for example, may read: “We found a math error on your tax return, and adjusted the amount of a credit you claimed, which changes your refund amount by more than $100. Please log in to see more details.”

### 10.2.4 Send more messages and take the time to build up trust

None of the above recommendations resolve the fact that the IRS is, as revealed in the user research, starting from a challenging baseline. Taxpayers are in general afraid to receive IRS communications. They have been taught that those communications will not come via the mediums they would prefer, and they are predisposed to expect any communications will be punitive. And indeed, this all maps fairly closely to the present reality that most IRS notices today do come in the mail, and are generally more likely to be about bad news than good.

These are undoubtedly obstacles. But our view is that the only way out is through. **The way to get taxpayers more accustomed to receiving IRS notices via email is to start sending more notices via email. The IRS may consider starting with easier, less controversial, less prone-to-misunderstanding types of notices (for example simple reminders to file), before moving on to any that have some complexities** (for example second-best automated returns, as discussed in Section 14.3.3). As the IRS sends more messages, people will learn to recognize legitimate messages and calls-to-action, and will better be able to distinguish them from phishing attacks.

The IRS shouldn’t become a spammer, sending multiple messages a week and dozens throughout the year. But erring on the side of more messages as part of a concerted campaign to build trust and get taxpayers accustomed to the communication is, itself, an end worth pursuing.

### 10.2.5 Use plain language and a friendly tone, and user-test communications

In written communications, to state the obvious, words matter. One way the IRS can make taxpayers more comfortable is by speaking in a way that inspires trust.

Direct File, indeed, received some feedback during its operations that its language had managed to alleviate taxpayers’ traditional fear of the IRS — language that was clear and specific, but that still treated readers like everyday humans, without retreating into jargon. This impression was not an accident: it was a function of a design team focused on striking such a tone, on providing the right amount of information at each point, and testing the wording with users to learn more about how it was being understood, and iterating accordingly.

Applying these same principles to other IRS communications — notices, emails, secure messages — will help taxpayers understand and trust those communications, too.

### 10.2.6 For further exploration: mass marketing campaigns

As noted above, some research participants mentioned they would better trust direct IRS messages and take more seriously new IRS offerings (e.g., Direct File) if they were also hearing about these topics via mass-media commercials. And, indeed, there is precedent for the idea that federal agencies ought to use advertising budgets to get their message out to everyday people.

On the other hand, mass marketing comes with its own complexities — and advertising and marketing are precisely those types of domains where there may be a gulf between what people say they will respond to, and what they actually do respond to.

It is worth considering whether paid marketing campaigns at the IRS would be advisable, though more research and investigation would be needed before moving forward with this idea. There also may be statutory bars to the IRS engaging in certain marketing activities.