Recommendations and Considerations for Electronic Services for Third Party Payroll Service Providers

presented by

NATIONAL PAYROLL REPORTING CONSORTIUM, INC. (NPRC)

ADP ★ AllianceHCM ★ Apex HCM ★ Asure Software ★ Check
CheckWriters ★ Dayforce ★ Gusto ★ Heartland Payroll Solutions
Intuit ★ isolved ★ Netchex ★ Paychex ★ Paycom ★ Paycor
Paylocity ★ PPI Business Services ★ PrimePay ★ Rippling
Symmetry Software ★ TriNet ★ UKG

January 2024

Table of Contents

Purpose of this Document 3
About the authors of this document 3
Recommendations 3
*CAPTCHA as a Security Tool 6
Contacting NPRC 7
References 7

Purpose of this Document

Nearly three million U.S. employers, representing more than 48% of the private sector workforce, use a payroll service provider (PSP) to electronically calculate, pay and file employment tax returns. PSPs often assist clients in resolving any problems or errors with such tax filings and payments as part of their payroll service. Generally, PSP interactions with a taxing authority are to submit information and tax payments on behalf of clients. The information flow is from the employer to the PSP, and then to the agency. After these submissions, tax authorities typically only return non-sensitive data to the PSP, such as confirmation that an electronic file was successfully received.

Due to the increased focus on data security, many taxing authorities are understandably concerned about releasing sensitive data to any potentially unauthorized recipients. PSPs have also increased their focus on data security and align with taxing authorities on the importance of data security. In addition, data and information security is an inherent part of the agreement between employers and their PSPs. However, some states seem to have over-compensated and are now restricting PSPs from performing certain high-volume batch operations on behalf of their clients. Now, employers using PSPs must increasingly follow diverse and complicated steps to comply with different state requirements in order to establish their intent to authorize a PSP to view their tax details and resolve tax notices.

Viewing employer-level tax details such as account balances, assigned employer tax rates, deposit schedules, historical tax deposits and historical employer-level tax returns are among the lowest-risk tier, especially if third-party users cannot view employee-level information such as SSNs and employee wages reported. Thus, requiring unique and/or difficult processes to establish authority to view employer-level tax details is unnecessary and in fact serves as a barrier to self service and data accuracy for employers that use PSPs. In addition, these complex processes deter the use of state web portals that were originally designed by state tax authorities to help employers and their PSPs resolve tax inquiries efficiently, through self-service, without needing to call the state.

About the authors of this document

The National Payroll Reporting Consortium (NPRC) is a non-profit trade association whose member organizations provide payroll, tax reporting, tax payment, and related services to more than 1.4 million employers nationwide, covering more than one-third of the private sector workforce. The NPRC actively supports appropriate electronic filing and tax payment programs. In addition to our long-time association and interaction with taxing authorities, we have long worked with the Internal Revenue Service (IRS), Social Security Administration (SSA), and state tax agencies to develop and improve standards for electronic systems.

Recommendations

The IRS, SSA, and most state tax agencies have made electronic services available to bulk processors, such as payroll service providers that often complete tasks in bulk on behalf of a list of clients. These services benefit the state agencies by enabling authorized self-service applications, which free up state personnel from handling routine requests via phone or written correspondence. These systems should include the ability to view transactions posted to client accounts, and can also include validation of assigned tax rates

and other critical details via bulk downloads, data exchanges, electronic copies of tax notices, secure messaging, and account resolution capabilities. These capabilities serve the needs of payroll service providers and other third party administrators such as accountants.

Some common obstacles/barriers with online tax agency portals, as well as official recommendations from NPRC, include:

- **Two-factor authentication (TFA):** TFA is an additional security step that can be implemented to ensure data and account security through an additional step during the log-in process. Typically this can be setup in a variety of manners: access codes sent to a specified email address, access codes sent via text and/or voice call, and sometimes access codes are sent through a mobile authentication application. Many PSP's security teams restrict users from using their personal mobile phones for conducting business. Allowing a code to be sent via email allows for the PSP representatives to retrieve the code using company-issued and approved computers/email accounts.
    - ***Recommendation:*** NPRC members prefer that the state offer an option to send a TFA code to an email address.
- **Employer access/visibility:** Some states don't offer any form of online employer access and/or are difficult to navigate.
    - ***Recommendation:*** State systems should be intuitive to navigate. In addition, state systems should enable employers to view their accounts online, to verify that returns and payments are being submitted by their PSP and were properly applied to their employer account.
- **Authorizations / Third Party Access (TPA) of PSP:** State agencies have a varying approach to authorization or TPA. Some agencies do not require authorization for PSPs to file/pay on behalf of their customers, and some agencies do require authorization to take these actions. For agencies that do require authorization, there is a wide variety of how this authorization is established. Some agencies allow "shared secrets" to be used in order to gain access. Shared secrets can be any information that the employer and payroll service could provide that's on record with the state, but that isn't available to the general public, such as the amount of one of the last three tax deposits. Some agencies require that PSPs request access and that employers then approve/deny the access request. Other agencies have an even more complex setup that requires multiple back and forth actions to be coordinated between the PSP and their client before authorization can be established.
    - ***Recommendations:***
        - Most importantly: Third-party authorization should not be required in order to file and pay on behalf of an employer since the PSP is only pushing information to the tax administrator during the filing process.
        - If third-party access is required for other actions beyond filing/paying (pushing information to the agency):
            - **Preferred approach:** the tax authority should allow PSP's to request access to the employer's account using "shared secrets" that are known to the PSP (such as: the Federal Employer Identification Number (FEIN), state account number(s), previous tax liability amount, previous wages reported, etc.). If the PSP enters these values correctly in the state

website, they should be granted access to view the employer's account immediately, without needing the employer to grant/approve the access. In this situation, the state could push a notification to the employer, to inform them that the PSP has access to view their account, and the state could provide instructions for how to remove access if the employer objects to this access.
    - **Example agencies with this functionality:** California Employment Development Department, Michigan Unemployment Insurance Agency, and Washington Employment Security Department.
- **Alternative approach:** the tax authority could notify the employer when a third party has requested access to the employer's online account, but not require that the employer approve or deny the request. After sufficient time has passed (i.e. 5 business days), if access hasn't been denied by the employer, then basic view and file/payment access should be granted to the PSP, in order to optimize usage of the online features that have been created.
- Additionally, employers should not have to enable TPA access requests before their PSP can request access. This enable/disable feature adds complexity to establishing authorization, blocks a timely TPA relationship from being established, and is cumbersome for all users involved.

- The website should also allow the employer to see who has been granted access to view their account so that they can manage third-party and internal users. The employer should be able to grant additional permissions (administrator roles, etc.) on an as needed basis.

- **Password Resets & Account Lockouts:** Experiencing password reset prompts is a natural part of accessing tax portals, and sometimes, account lockouts occur. In some situations, when a user is locked out of an agency website, the agency will require that the primary administrator of the PSP's profile call to get the account unlocked and to prompt the password reset process. This restriction in terms of who can contact the agency to get the account unlocked can postpone resolution of the issue at hand.
    - ***Recommendation:*** For large PSPs, it would be helpful to allow multiple administrators, so multiple team members can call to get the account unlocked and to prompt the password reset process to the email address that's already on record for the PSP.
- **Administrator Changes:** Many state websites require that a primary administrator be appointed on the PSPs account/profile. Due to natural turnover within a PSP company, sometimes this primary administrator needs to be changed. Some state websites don't allow the administrator to be updated, resulting in all employer clients needing to be reauthorized under a new administrator, even though the clients are still using the same PSP to process payroll. Other state websites have a complex process for updating this administrator, that involves filling out forms, submitting them to the state, and waiting for them to be processed before the administrator can be updated.
    - ***Recommendation:*** Enable a seamless process that can be completed within the PSP's profile, for a quick administrator transition. Most importantly, allow for the ability to

change administrators when there are role changes at the payroll firm without needing to reauthorize all employer-clients under the new administrator.

- **System Performance for PSPs:** For some state websites, PSPs experience extreme slowdown once they've added several hundred or several thousand clients to their profile. At times, the slowdown renders the websites to be useless for the PSPs resulting in more phone calls and emails to the state agency.
    - ***Recommendation:*** Consider the system performance of the web pages that display multiple employers. Monitor page load responsiveness and make routine enhancements to ensure the website is performing as expected.
- **Security protocols:** In order to bypass security measures used to identify fraud and to deter usage of automated transactions from unknown parties, some state websites utilize security features that may not be appropriate for large and known PSPs (that need high-speed automation capabilities).
    - ***Recommendations:***
        - Implement IP address accept listing or allow listing in order to permit high-volume automation from known and trusted TPAs. Avoid the use of CAPTCHA* for high-volume transmitters, such as PSPs *(see section below regarding CAPTCHA).*
        - Allow for the exchange of secure keys.
        - Leverage the use of APIs for trusted third-parties to enable the automated exchange of approved information between the tax authority and the PSP.
            - Example: California's data exchanges via web services which allows for the real-time exchange of information from approved PSPs.
- **Employer search criteria:** When PSPs log into state websites to access their clients' records, some state portals feature restricted search-functions. Most portals only require PSPs to enter the Federal Employer Identification Number (FEIN), the last four digits of the company FEIN or the company name. More restricted portals require PSPs to enter in an "Account ID" or some other identifier which is a different number than the numbers used for filing payroll-related taxes, such as the employer's FEIN and is a different number than the employer's state EIN. These Account IDs are not used for payroll tax filing nor deposit functions. Most PSPs don't obtain their clients' Account IDs, so they have no way to locate their clients in the state portal. In addition, employers have general confusion about the difference between Account IDs and state EINs.
    - ***Recommendation:*** Expand the search capability function of state portals to include FEINs, state EINs, company names. Do not just use the Account IDs or other identifiers that are not used for payroll and therefore not available to PSPs.

*CAPTCHA as a Security Tool

- CAPTCHA is a tool that is added to a web page to determine whether a user is a bot or a human. It invokes a confirmation measure known as challenge-response authentication, by asking the user to complete a simple test that proves you are a human. Typically, these come in the form of a distorted series of letters and or numbers or images to be selected based on a prompt.
- However, all CAPTCHA can confirm is that the person accessing the CAPTCHA sequence is a person and not a bot. It can't validate that the person is who they say they are and is therefore not really

a security measure as it doesn't provide an answer to a significant security question: "is this a trusted person for this site."

Contacting NPRC

NPRC members are very interested in working with all state tax authorities to develop secure and functional online tooling for viewing and performing actions on taxpayer accounts. Please let us know how we might assist in addressing these issues. If there are additional questions about online tooling, please contact NPRC at nprc@nprcinc.org.

References

Rutter, T (2005) CAPTCHA are not a security measure

Pankov, N (2021) RIP, CAPTCHA

Young, L (2021) Building a WebAuthn Click Farm - Are CAPTCHAs obsolete?