Best Practices for Summer EBT Self-Service Portals

Introduction

Summer EBT, sometimes referred to as "SUN Bucks", is a new, permanent child nutrition program administered by the US Department of Agriculture (USDA), Food and Nutrition Service (FNS) to provide food assistance over the summer to children who typically receive meals at school through the use of an electronic benefit transfer (EBT). In 2024, the implementing states, territories, and Indian Tribal Organizations (ITOs) estimated that they would serve almost 24 million children.

Eligibility for Summer EBT consists of a streamlined component that attempts to automatically include as many children who are known to meet the income requirements without the need for further application. However, applications are still required from some families, and the information that is on file for streamlined certified cases may need to be updated. Despite the program's emphasis on issuing benefits automatically to as many eligible children as possible, families may frequently need to interact with Summer EBT implementing agencies in order to understand eligibility rules, check their childrens' statuses, update their contact information, and engage in other program-related administrative functions.

Many of these tasks are commonly considered customer support, and can be addressed by staffing a customer support call center. However, the actions clients must take are often quite simple, and empowering clients to resolve their own issues through the use of technology can be a more cost-effective and timely solution than relying on a call center as the front line for customer service. One powerful tool for client-directed benefits management is a self-service portal for parents, students, and families.

A self-service portal is a web-based system that enables people to take care of common Summer EBT tasks themselves, such as checking the status of streamlined certification, application, or card issuance; updating personal information such as mailing addresses; or creating support requests for complicated procedures, like verifications and appeals.

Self-service portals for Summer EBT offer benefits for both families and government staff:

- For families with children who may be eligible for Summer EBT, a portal allows parents to conveniently access and manage key information about their child's eligibility and benefits.

- For government staff, a portal reduces the need to respond to inquiries that could be quickly resolved via self-service, reduces the number of cards that are returned as undeliverable, and decreases the likelihood of applications being submitted that are duplicates of streamlined certified cases.

Self-service portal prioritization

There are many areas that Summer EBT agencies can invest in as their Summer EBT services mature. To determine whether building a self-service portal is worth prioritizing:

1. **Assess how much of your current workload a self-service portal might be able to reduce**

   - Analyze the volume of requests and inquiries related to Summer EBT service needs that could be self-serviceable, including calls or emails to check the status of a child's Summer EBT benefit or to update household contact information.

   - Count the number of applications filed for children who are already streamlined certified.

   - Evaluate whether support teams have the capacity to manage the tasks these requests generate manually. If these requests regularly overwhelm staff, a portal may reduce the workload and improve response times.

2. **Conduct user research**

   - Test potential self-service solutions on program participants by conducting user research, ensuring that proposed solutions meet actual customer needs. **Code for America's Qualitative Research Guide** has helpful tips and guidance for conducting research with participants.

   - If the empirical data on support issues mentioned above isn't available, you can conduct surveys to help fill in knowledge gaps.

3. **Evaluate internal resources**

   - **Data and policy**

     ▸ Do you have the data you need to authenticate parents/guardians and to associate them with their children? This data allows you to provide functionality to families as a whole, rather than child-by-child.

- If you don't have access to parent/guardian data linked to children, then more privileged functionality, such as modifying a mailing address, might require the verification of the identity of the eligible child; for example, this could happen by providing a copy of a birth certificate and/or Social Security card. Due to the high burden of providing this information, it may make sense to deprioritize some functionality until that data can be obtained. This might involve modifying school directory information notices, creating new opt-out forms, or adding data-sharing permission questions to benefit program applications.

- Can you link parents/guardians to children using data from streamlined certification? If family relationship data for some children isn't available, it may still be worth prioritizing more advanced functionality for those households where your data allows you to link parents/guardians to children. For example, if household composition information is available for all children who are streamlined certified via Medicaid and SNAP data but not for children certified based on school data, it could still be valuable to provide the ability to supply a mailing address and other advanced functionality to those households, while providing more basic status checking functionality for all.

- **Review your current technology**

  - Assess whether your existing technology infrastructure can support a self-service portal. This includes evaluating how easily your systems can connect with databases that handle streamlined certification, application, and Summer EBT program data.

- **Consider funding and staff**

  - Evaluate the funding opportunities available for tech and data related work.

  - Ensure that staffing for internal resources or budgeting for external resources can meet the support needs to research, design, implement, maintain, and operate the portal.

- **Invest in program and project management**

  - Ensure development teams follow an agile development process. A self-service portal, like any other developed product, will require iteration based on what you learn about user needs and preferences. An agile development approach is an effective way to efficiently and effectively tailor product specifications to user needs. See more about agile development practices in **18F's De-risking Guide**.

  - Be prepared to assign program management roles to staff who will have continuous visibility into the portal's status, maintain alignment with big-picture and small-picture goals, keep communication between teams fluid, and manage relationships with other stakeholders within your organizations. It may be valuable to budget additional staff for these functions.

  - Confirm that a product owner can serve as a dedicated resource to oversee the success of a development project and reduce risk. See more about empowering a product owner and their value in **18F's De-risking Guide**.

Core principles for a user-friendly, effective self-service portal

One of the first steps in building a self-service portal is to enumerate the functionality it should support and sketch what it might look like. This section gives some principles to use in the design process to ensure that the finished result meets client and agency objectives.

Human-centered design

Human-centered design prioritizes the perspectives of the people for whom the product is being made. For a self-service portal, it is complemented by *user-centered* design which attempts to have the technology adapt to people rather than the other way around. They stand in contrast to design practices that focus on systems, technologies, or even specific sets of functionality that are not well calibrated to real-world applications. Interviewing parents about their experiences managing benefits and performing usability tests to capture feedback about how users interact with the portal are two of several methods that can help government staff prioritize the design of a portal to ensure it meets the needs of the people using it. See **18F's De-risking Guide** for more details.

User experience

A user-friendly self-service portal should prioritize simple navigation, reduce the steps it takes to complete tasks, and accommodate the needs of end users. Examples of accommodation include—but are not limited to—supporting translations for multilingual users, ensuring accessibility for users with disabilities, and building responsive designs to adapt to users accessing the portal across different device types (e.g., smartphone, tablet, desktop). See **Code for America's Benefits Playbook** for user-friendly principles for benefit application designs, and **18F's User Experience Guide** for more details.

Clear communication

Transparency in designing a self-service portal builds trust and ensures end users have a clear understanding of their actions and benefits. Providing real-time information is crucial to supporting the needs of end users and reduces the reliance on government contractors. Anything from a confirmation message when a parent updates an address to a notification about a status change can impact the user experience. Additionally, offer clear instructions and explanations throughout the user journey, helping end users understand what actions they need to take, what is happening with their benefits, and how long it may take to issue benefits.

Feedback and support

Providing opportunities for feedback and support is essential for continuous improvement and ensuring users get their questions resolved. Portals that include feedback mechanisms, such as a dedicated widget or form where users can report issues, suggest improvements, or provide general comments about their experience, are commonly used across web-based systems. However, before deciding to collect feedback, consider whether government staff have the capacity to implement it. We don't recommend collecting feedback if there are no plans to follow up with users individually to resolve issues or use the feedback for broader program improvement. Additionally, it's important to offer clear access to support options, including FAQs, knowledge bases, and contact information

for live assistance. Although the goal of a self-service portal is to ensure users can find answers to their questions autonomously, providing clear instructions on how to access additional support will help users resolve issues if self-service functionality cannot support them.

Key user-facing components

The features below highlight common user needs heard from discussions with states and tribal nations. Not every self-service portal will or should include all of these features. Your portal should be scoped to address the most pressing needs of families and to make impactful reductions on staff support needs.

1. **Eligibility screening and application status tracking**

   a. **Description**

   - Clearly presented information about the eligibility status of a child and/or the status of an application.

   b. **Key features:**

   - **Checking whether a child is already on a streamlined certification list:** Parents and guardians are less likely to submit unnecessary duplicate applications if they can easily learn that their child is already certified for Summer EBT. A best practice is to allow users to check whether their children are included on the state's eligibility list by matching against student information. Since the user's core questions are "Will my child get benefits? Do I need to apply?" and since the agency has definitive enrollment information for a large majority of eligible children, an individual eligibility checker that matches students to the state's existing certification list is likely a more effective solution than a generic screener.

     The precise information you can use for matching will be determined by the student data you have available, but many students will likely be able to match based on information that is easy for parents and guardians to produce, such as a combination of the child's name, date of birth, and school or ZIP code. Illinois's Summer EBT screener uses language that avoids a definitive statement about eligibility, to avoid exposing program participation information (see Figure 1).

   - **Checking the status of a submitted application:** Because it's possible for households to apply for Summer EBT months before benefits are delivered, application status checkers are valuable throughout the year. Some commonly used terms to describe an application status are:

- ▸ *Submitted:* the application has been submitted from the user's end but has not been reviewed by eligibility workers
- ▸ *Under Review:* the application is under review by eligible workers
- ▸ *Approved or Denied:* based on the eligibility criteria of the program
- ▸ *Additional Verification Needed:* requests more information from the applicant before a benefits issuance can be made
- ▸ *Under appeal:* if applicable
- ▸ *Pending:* applications that are received early in the school year before enrollment data is available

- **Opt-out functionality:** Families who were streamlined certified should be able to opt-out from Summer EBT using the portal. Using best practices from **psychology** for effective communication, make it clear that clients are entitled to the benefit and it is something that they already "own", e.g. "To opt-out of receiving your SUN Bucks, click here." It should also be clear that receiving Summer EBT does not impact eligibility for other benefits, depend on or influence immigration status, or have tax consequences. Clients should be prompted to confirm their choice. Since opting-out should be rare, it may be worth soliciting feedback from clients at this point regarding their motivations.

c. **Design considerations**

- **Use plain language:** Use terms that both government staff and end users can clearly understand. For example, while agency staff may use "streamlined certified" to identify children that are already eligible and do not need to apply for the Summer EBT benefit, parents and guardians may be unfamiliar with the term. It's easier for users to understand familiar, plain language terms like "pre-approved" or descriptive explanations like, "We already have the information we need to determine [NAME's] eligibility."

- **Give clear instructions on the actions users might need to take:** When users need to take an additional step, such as submitting an application or calling a support line when a screener doesn't return a positive match for eligibility, use simple, action-oriented language to convey the next steps they must take. Use design features to make it easy for users to take actions that could connect them to benefits. For example, use a distinct, large "apply now" button or a direct pathway from a screener into the application flow to connect users to an application as quickly as possible.

- **Make it mobile-friendly:** Clients come to Summer EBT primarily from their phones, so making a mobile-friendly self-service portal is critical. According to Nutri-Link, creator of the USDA-sponsored Summer EBT application platform, about 85% of application submissions are from mobile devices. For information on building a mobile-friendly site, see **Code for America's Benefits Playbook**.

d. Sample screener results pages

Figure 1: The result of child lookups in Illinois (top) and New Mexico (bottom) Summer EBT screeners. The system gives the determined status if possible, and otherwise indicates that the child could not be found. The Illinois screener also echos back masked contact information.

2. Verification and appeals

a. Description

- For households selected for verification or who chose to appeal a denied application, a self-service portal can convey case status, indicate next steps, and allow clients to take action.

- Critically, a mobile-friendly portal can include an easy way to **submit documents to the agency using their phone camera** or their computer for the sake of satisfying verification requests or providing documentary evidence in support of an appeal.

b. Key Features

- **Secure information about required verifications:** After authentication, give families whose applications have been selected for verification as much relevant information as possible. This includes:

  - ▸ copies of paper notices
  - ▸ information about the types of verification documents required
  - ▸ deadlines for submissions
  - ▸ examples of the kind of verification documentation that is likely to be acceptable
  - ▸ a log of when and how the agency makes its attempts to contact
  - ▸ guidance on how to submit verification documents, ideally through the site itself
  - ▸ status of any verification requests, including an indication when documents have been received and are in review
  - ▸ functionality for families to provide collateral contacts if written evidence cannot be provided

  See the USDA's **Verification in Summer EBT** for a succinct summary of verification guidance and **Best Practices in Developing Effective SNAP Client Notices** for how to convey administrative action notices.

- **Accessible document uploading:** For ease of access, a best practice is to allow users to upload documents without logging in. Because verification or appeals will only be required for a small number of users—all of whom have submitted applications— agencies can distribute unique links to clients to help associate documents with individual applications.

- **Appeal functionality and guidance:** If applicable, a self-service portal should contain the ability to file an appeal on a denied application, with similar functionality to that developed for verifications. It should also convey appeal-specific information. In particular, in the case of a denial for verification, the self-service portal should provide the documents and records that support that eligibility determination.

3. Secure login/authentication system

a. Description

- This allows users to log in, validate their identity, and access advanced self-service functionality.

b. Key features

- Protects self-service features that require a higher degree of assurance regarding the identity of the user. See the **Authentication section in this document** for more details.

## 4. Central dashboard

a. Description

- This is a central location that serves the parent key information about eligibility, status updates, action items, navigation links, etc.

b. Key features

- **Household-level view:** If parent or guardian information can be linked to children and can authenticate as the head of household, they should be able to view all their children's cases together. The portal can also allow users to apply changes (such as address changes and contact information updates) to one or many of their children at once.

- **Most frequently accessed functionality:** The central dashboard should provide straightforward access to the most commonly utilized actions from user research or client support metrics.
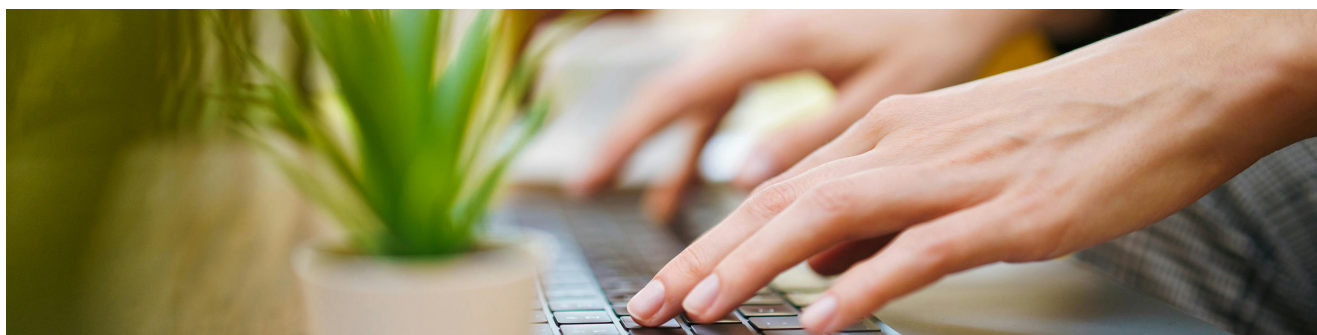
5. Card and benefit tracking

a. Description

- This is a report that displays information about benefits issuance, and includes the capabilities to request a new card if needed.

b. Key features

- Reporting information should include whether benefits were issued (yes, no), where benefits were issued (last 4 digits of the card to protect card information), the current balance of the card, the date of last issuance, and date of expungement.

- Users should have the capability to request a new card if necessary. Here's an example workflow of what this could look like in practice:

  - ▸ User initiates a new card request through a widget in the portal
  - ▸ Confirm with the user whether the card was lost or stolen
  - ▸ Inform user of implications of requesting a new card, including any notable updates to expungement that may occur as a result of ordering a new card
  - ▸ Inform the user of the lost or stolen card deactivation processes, such as the automatic deactivation of a card once a new one is requested
  - ▸ Confirm the mailing address for card, asking if they want the card shipped to the mailing address on file or an alternative mailing address
  - ▸ Inform the user of expected delivery times and any required next steps
  - ▸ Enable the user to track the status for card replacement requests, similar to package tracking (e.g., request received, card shipped, estimated delivery)

- Users should also be able to request replacement benefits for food purchased with Summer EBT benefits that were lost to household misfortune or disaster

  - ▸ Have a user-friendly way for clients to submit whatever evidence might be required
  - ▸ Indicate to clients the status of their benefits replacement
  - ▸ Once a determination has been made, show the outcome to the clients and indicate any relevant dates or amounts

6. View and update contact information

a. Description

- This means a form that allows users to update contact and address information on file.

b. Key features

- Provide visibility to current contact information on file, including the name, phone number, email, and mailing address. Using autofill functionality to surface this information to users helps reduce the chance for data entry errors.

  - ▸ For limited forms of authentication, allow this information to be echoed to clients with the majority of its content obscured. For example: a phone number ending in XXX-XXX-1234.

- Allow users to edit all contact information in one click, with the ability to save and overwrite information in case of a data entry error.

- Implement real-time validation to prevent common errors like typos or invalid addresses. This can be done using a postal address verification API, such as the USPS address verification or Smarty.

- Validate phone number and email entries in real time to reduce data entry errors. For example, if the email address field does not include an @ in the form field, the submission should surface an error to the user and give them information about why it has failed. Applying a similar concept to phone numbers, ensure phone numbers follow a standard format such as XXX-XXX-XXXX

- After submitting changes, users should receive an on-screen confirmation and an email notification detailing the update. Confirmation messages ensure transparency and allow users to verify that the system recorded their change correctly.

- Given the sensitivity of address and contact information, features to submit changes should require a higher level of authentication, such as the multi-factor authentication (MFA) approaches detailed in **Authentication** below.

- For families with multiple children, the portal should allow users to select which children the mailing address update should be applied to or to apply it to all children simultaneously. This avoids the need for redundant submissions, reducing errors and improving efficiency.

7. Knowledge base/How to connect with support

a. Description

- This is a section that provides users a space to read FAQs, knowledge base articles, and contact support channels.

b. Key features

- FAQs should centralize questions users commonly ask, and are intended to provide insight into more general questions as opposed to case specific inquiries.

- Knowledge base articles include deeper dives into questions about eligibility, benefits issuance, support, etc.

- Contact information includes detailing phone numbers, emails, or links that guide users to support channels available for further support. Details should also include days and times staff are available to support users.

8. Digital communications

a. Description

- This is the functionality to send communications to end users.

b. Key features

- It's necessary to generate messages from the portal to reach all, or select, end users. Examples include notifications and in-portal banners notifying users that an application deadline is approaching, or informative messaging about the time window to expect benefit issuance.

Authentication

For many common self-service functions, authentication is the first step of a user journey in accessing a Summer EBT self-service portal. Most Summer EBT benefits are issued automatically on behalf of children without the need for parents or guardians to create an account. As a result, authentication for a Summer EBT self-service portal serves two roles: finding relevant records and establishing proof of identity for the person trying to access self-service functionality.

Correspondingly, there is information that can be made available to clients through a self-service portal after a simple records search, and other functionality that should require identity verification. It is important to note that gating less sensitive information behind aggressive authentication schemes can dramatically decrease a self-service portal's utility.

Background

1. User profiles/scenarios

A well designed self-service portal can provide a lot of functionality that parents and guardians may want to access for their households' Summer EBT benefits. Here are a few scenarios in which such a portal could help people receive their Summer EBT benefits amid complex household circumstances:

- A family has two children who attend different schools, one of whom applied for and received free/reduced-price (FRP) meals while the other attends a Community Eligibility Provision (CEP) school. The family should be able to see that one of their children will automatically receive benefits and the other will need to apply. They have no contact information in the system, but are able to access limited portal functionality—including their children's statuses—by supplying their childrens' names, dates of birth, and address.

- A family experiencing housing instability has moved frequently throughout the school year and does not have their current address on file with their school. They should be able to supply the address where they want their card mailed before it is issued. To do so, they request an email be sent to an account they maintain that contains a link they can follow for a one time login.

- In a split-custody family, one parent has claimed a child for SNAP while the other is the primary caregiver and is registered in school data. The primary caregiver should be able to enter their child's identifying information directly and see that the child is already set to receive benefits, but not where the benefits will be sent. They should also be able to authenticate using parent/guardian data supplied to the school and see that no children are linked to their account. From the portal, they can contact support to start a resolution process and claim their child.

In contrast, the following are use cases that a self-service portal should protect against:

- An ex-partner involved in a domestic dispute should not be able to re-route the card from the address on file using just their knowledge of the head of household's contact information. This is ensured by requiring a factor of authentication beyond knowledge to make an address change, such as a text message with a one-time code.

- An ex-partner or any user should not be able to see complete contact information without establishing their identity to obtain an appropriate level of access.

- It should not be possible for information to be obtained by repeatedly entering publicly available information, like that from voter registration files. To prevent this, rate limit access from a single IP address and use professional bot prevention services.

2. Levels of access

There is little inherent risk in determining whether a state has enough information to assess a child's eligibility, because Summer EBT is a program that reaches many children, often automatically through streamlined certification. It is also possible to allow parents to see if they need to supply a new mailing address for streamlined certification while preserving their privacy. This can be accomplished by relaying the generic source (e.g. "school" or "assistance program") of the address on file and when it was most recently verified. We believe the value in making this information easy to access outweighs the potential harms and should be made available through what we call "unauthenticated access," described below.

3. Family vs. child access

If you are able to construct full-family information from streamlined certification and school enrollment data sources, it is possible to allow a parent/guardian to authenticate directly. Parents/guardians usually have more options for rigorous authentication than children, so it's easier to establish trust, and a portal designed around families allows them to see and operate all of their childrens' cases at once. This kind of access is complicated by the fact that only head of household information may be available, and—in particular with split-custody families—there may be conflicting information assistance programs or school registrations. As such, always have an option to look up the statuses of individual children.

Types of authentication

Authentication systems **generally use** some or all of these three types of information to verify that a person trying to access a system is who they say they are:

- Something they know (e.g., a password or unique and private identity data)

- Something they have (e.g., a case number, a phone number, or a cryptographic key)

- Something they are (e.g., a fingerprint or other biometric data)

For Summer EBT, state agencies already possess a lot of information that parents or guardians know and have that might be used to authenticate them into a self-service system. Agencies can also use account creation after a Summer EBT application flow to create new authentication pathways. *Note: We strongly recommend that states DO NOT require people to log in to accounts before completing and submitting Summer EBT applications.*

1. Unauthenticated access

The goal of unauthenticated access is to give a reasonable degree of confidence that a person is representing themselves truthfully without being overly burdensome, and is applicable for seeking information that would be of relatively small privacy risk if it were disclosed. The information obtained from clients for unauthenticated access is primarily used to identify the unique record that corresponds to that individual. One foundational study in privacy research found that **87% of individuals** can be uniquely identified by their ZIP code, gender, and date of birth, so only a few data elements should be necessary for most cases. For example, a client might be prompted to enter three out of the following:

    a. **Legal last name**

    b. **Birthdate**

    c. **Last four digits of Social Security number**

    d. **First address line from school registration**

    e. **ZIP code**

    f. **Phone number**

    g. **Email**

Figure 2 illustrates some real-world examples, including New Mexico's "Let's Check Your SUN Bucks" site and Illinois's Summer EBT Screener. Also shown in Figure 2 is South Carolina's **SNAP/ TANF Benefit Inquiry Portal**, which allows access with a case or card number.

When asking for this kind of identifying information, it is important to note that names are often supplied in a variety of ways, addresses often become out of date, and a wide variety of other errors are commonly made. Incorporating probabilistic or fuzzy matching rules can help address this so parents don't have to guess how they might have written down their name on a school form. If this results in multiple records matching, simple follow up questions can solicit additional information.

Unauthenticated access corresponds with **NIST Identity Assurance Level 1** (IAL1), and is colloquially referred to as "something you know."

Figure 2: New Mexico's Summer EBT (top) and Illinois' (middle) student streamlined certification portals. For New Mexico's portal, parents/guardians can see their child's status by entering their name, date of birth, ZIP code, and optionally, a student information number. For Illinois, parents/guardians must enter either their name and date of birth, or Social Security number and one other piece of identifying information. Optional fields help reduce the likelihood of multiple matches. On the bottom is South Carolina's SNAP/TANF Benefit Inquiry Portal, which utilizes date of birth and card or case number.

2. Light-touch authentication

A light-touch approach to authentication remains easy for most clients to navigate but provides states with a higher degree of confidence in the result, and is appropriate for revealing more sensitive information and making changes to cases. It often involves an additional factor of authentication after identifying information has been provided. User-friendly examples of this include:

- Text, call, or email existing contact information with a **magic link**

- Log in through a state single sign-on (SSO) provider or **social login**, such as Google or Apple

- Text, call, or email existing contact information a one-time verification code (this can be less preferable for **accessibility** reasons)
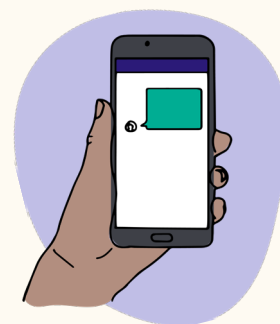
Another client-friendly way of accessing the site is to allow access from the client portals of the programs used for streamlined certification.

For the most part, light-touch authentication corresponds with **NIST Identity Assurance Level 2**. The additional factors of authentication incorporate "something you have."

3. Heavy-touch authentication

When all of the contact information on file for a family is no longer accurate, it might still be beneficial for families to have a way to prove their identity and access self-service options. Because the bar to establish trust without the ability to utilize an additional authentication factor is quite high, methods in this category can be extremely onerous and **difficult for clients to navigate**; they should only be required when identity cannot be verified using simpler means. Examples of heavy-touch authentication include services like ID.me, knowledge-based verification providers like those provided by credit bureaus, and other forms of **Remote Identity Proofing**.

If data quality concerns exist such that you think there are many cases with children who are not linked to parents or guardians, and where there is a strong need for a specific, privileged self-service option—for example a large body of students with no address information—allowing parents/guardians to claim children by submitting copies of birth certificates, Social Security cards, or photo identification may be useful. We do not expect this to be necessary in most cases.

Other authentication concerns

1. Accounts and passwords

Requiring clients to create accounts or recall passwords before being able access information can represent a significant **usability barrier**. If creating an account would allow for significant additional functionality, explain the benefits clearly to clients and offer a number of ways of establishing one. For example, using a single-sign-on identity provider such as **login.gov** can allow the client to access multiple services if it is already in use in a state or ITO. The multi-factor approaches listed in the light touch authentication strategy section above effectively allow for account creation in a way that is invisible to clients, as they can always log in through one time use tokens or SSO.

2. CAPTCHA

CAPTCHA—completely automated techniques to ensure that web traffic comes from humans—are often significant **accessibility barriers** to clients. As the goal of a CAPTCHA is usually to prohibit procedural access to servers, alternatives such as **rate limiting** and/or geo-location can be employed. In addition, the security industry offers a number of approaches to detect and mitigate bot traffic in a way that is largely invisible to most end-users, such as CloudFlare's **Bot Management** service. It can also help to build into your business processes alarms that trigger on suspicious activity, such as a large number of cards being redirected to a single address or area with a relatively small number of postal delivery points.

Evaluation of authentication strategies

Authentication should be evaluated in terms of how difficult it is for clients to complete against the privacy and legal risks of unauthorized disclosure. Those interested in a formal approach to evaluation can implement the **NIST Privacy Risk Assessment Methodology**, a set of worksheets that allow an organization to identify, quantify, and prioritize privacy risks. While directly measuring the harms of improper disclosure to clients can be complicated, the harms of a lack of access are more directly quantified:

- How often do clients have to reach out for support? How long are they on hold or how often do they have to call back? How often are there delays in obtaining benefits?

- How much time does support staff have to spend addressing client questions? How many cards are undelivered?

- Specifically with regards to authentication: How many failed authentication attempts do you see that appear to be from legitimate users? How many password reset requests or tech support calls do you receive? How much time do users spend at the authentication screen?

The risks of any authentication strategy always involve tradeoffs between ease of access and possibility of disclosure, and the key to a risk-management strategy is being able to align your organizational priorities with those outcomes.

Table of authentication risk levels

Below, we outline some core functionalities as described in the **previous section**. Refer to that section for recommendations on the required authentication levels for clients to access these functions.

Function	Potential risk level	Notes on risk
Change address for card delivery	High	Could enable bad actors to re-route EBT cards away from households
See current address on file for card delivery	Medium	Could expose sensitive location information of households fleeing domestic violence
See provenance of current address on file for card delivery	Low	It may be enough for families to know where the address comes from (e.g. "school" or "benefits") and when it was last verified
See EBT card balance	Medium	
See date of EBT issuance and expungement	Medium	Stating the issuance and expungement schedule is a zero-risk way of addressing this
See which card will be issued benefits (existing or new; if existing, which card)	Medium	Exposes information about household income that a household might consider sensitive
Request a replacement card (if address has recently been changed)	High	Could enable bad actors to re-route EBT cards away from households
Check application status (received, in-process, processed)	Low	This can be further de-risked by requiring an application confirmation number
Check streamlined certification status	Low	Might expose information about household income that a household might consider sensitive; can be de-risked by not indicating the source of streamlined certification eligibility
See whether additional verification is needed	Medium	Could expose information about household income that a household might consider sensitive, but note that selection for random verification is not privileged information
Submit verification documents	Low	
Update/add contact info (phone number, email address)	Medium	Using one existing piece of contact information as an authentication factor before changing a different one helps ensure identity