Washington State / Notify.gov

Case Study Outline

Drafted: Aug 2024

Created by: Emily Herrick - Q2AAFDA

Reviewed by: Cathy Beil - Q2AAFD Washington State*

*Washington State has reviewed, edited, and approved this outline as talking points. If we are creating a written post / publishing publicly we will need to send any final version to Washington State again. Point of Contact: Donald Paul, donald.paul@dshs.wa.gov

Problem context

Like many SNAP recipients nationwide, participants in the Basic Food program in Washington state have lost vital access to food benefits through EBT card skimming and cloning.

- From April 2022 to June 2024, nearly 9,000 customers reported losing $5.5M in benefits.
    - As of July 31, 2024, Washington has reviewed over 9,500 claims and replaced $3.4M in food benefits.
- Policy and card infrastructure are chipping away at the problem of EBT skimming, but policy change is slow.
    - Chip cards are more secure but costly. A federal bill was introduced to require chips in EBT cards nationwide. States such as California and Oklahoma, among others, are testing EBT chip cards this summer.
    - FNS mobile payment pilot is expected to launch in five states.
    - Stakeholders are pushing Congress to extend the federal reimbursement authority, which is set to expire in September – and they also require and fund the widespread adoption of EBT card security.
- As we wait for policy and technology infrastructure to change, Washington state has taken a proactive fraud prevention strategy.

Washington's proactive fraud prevention strategy

The Washington State Department of Social and Health Service has taken a proactive approach to preventing, detecting, and mitigating these thefts.

- In 2022, the agency increased data analysis to detect skimming or potential skimming early. Using this data analysis, DSHS identifies cardholders at risk for potential theft.
- Since these benefits are so critical to families, DSHS initially attempted to contact cardholders by phone to help them replace their cards as soon as possible, but this process is time-consuming. If DSHS is unable to get ahold of them, it will take the following action:
    - Mail a letter to the customer to identify that their card is compromised and advise them of actions needed to protect their benefits.
    - If the customer does not act after 12 days, then the card's PIN is reset, requiring another letter to be sent to the customer advising them of the action taken. This is a key step that helps prevent benefits theft but also prevents the recipient from accessing those benefits.
- Where texting fits in preserving benefit access *and* preventing theft
    - DSHS works to identify compromised cards before benefits can be stolen. If a compromise issue is identified before benefits are issued to the card, the

team can sometimes prevent theft by deactivating or changing the PIN on that card. However, recipients are then blocked from accessing their benefits until they replace their card.

    - By adding a text message, DSHS can send notifications allowing customers to immediately take action that preserves access to their benefits while preventing theft.

About Studio/Washington partnership

DSHS sought to reach people more reliably and reduce the need to put up barriers to benefits. It partnered with the U.S. General Services Administration's Public Benefits Studio to pilot Notify.gov, which sends text alerts to affected beneficiaries.

- Goals for EBT cardholders
    - Maintain access to benefits; it's not just about catching criminal actors for customers — It's about having your benefits when you need them, as you anticipated and expected.
- Goals for Washington
    - Understand the effectiveness of texting as a mechanism to contact cardholders more efficiently and effectively and help them understand what safeguarding actions to take.
- Goals for Studio/Notify.gov
    - Support using agencies:
        - Understand what support and information benefits agencies need to send effective text messages.
        - Scale an easy-to-procure technology product and then use it.
            - Test the usability and functionality of Notify.gov.
    - Support cardholders:
        - Understand the value of texting in the context of a client's life.
        - Gather evidence of texting's impact on programs and participants.

Building a texting campaign

- We took a shared design approach to the Washington pilot campaign. We wanted to understand what problem we were trying to solve, how we typically contact our customers, and our assumptions about how texting could improve customer experience.
- Through a series of collaborative sessions, we designed a campaign with the following components:
    - Identified audience and desired action.
    - Created message drafts.
    - Planned outreach.
    - Sent and tracked messages.

Identified audience and desired action

- Together, we drafted a hypothesis that informed the design of the texting campaign:
    - We believe texting EBT cardholders once we determine their cards are compromised can help prevent them from experiencing lost cash and food benefits due to fraud.
- We also discussed the desired impact of this communication campaign:
    - Prevent lost benefits and ensure program participants receive the funds rather than criminal actors.
        - If Washington sends a text before benefits go out, it gives cardholders time to take safeguard actions before their benefits are stolen.
    - Demonstrate that the state is taking action to safeguard customers.

Created message drafts

- Our hypothesis and desired impacts grounded what was important to include in the text message content.
    - For fraud prevention, there are several safeguarding actions a client can take, from getting a new card to changing their PIN or temporarily locking their card.
    - All are important, but a text message is a small amount of real estate, and Washington didn't have much space to tell people about all their options.

— This could also lead to choice paralysis, so Washington got as specific as possible about what key action it wanted text recipients to take.
    - Customers need to get a new card. Those receiving the text had already been flagged at risk for potential theft, and getting a new card was the best way to safeguard against future fraud. Other actions were temporary and reversible.
- A big, open question the team discussed at length was whether we should include the actual phone number in the text or not. Washington was hesitant about how to direct people to action without giving criminal actors opportunities to attempt to collect customers' personal information by spoofing. The cybersecurity term *spoofing* is defined as pretending to be someone else to steal data or money or to spread malware.
    - After a few content iterations, the team decided not to include the phone number in the text, instead advising individuals "to call the number on the back of their card." While this may still deter people from taking action, Washington thought it was important to create the most fraud-resistant message possible.
- *Washington DSHS: We've identified unauthorized use on your EBT account. Call the phone number on the back of your card to cancel or go to your local CSO for immediate replacement.*
- Additionally, because Washington has language preferences for customers on file, it was able to translate the final message into 16 different languages in addition to English.

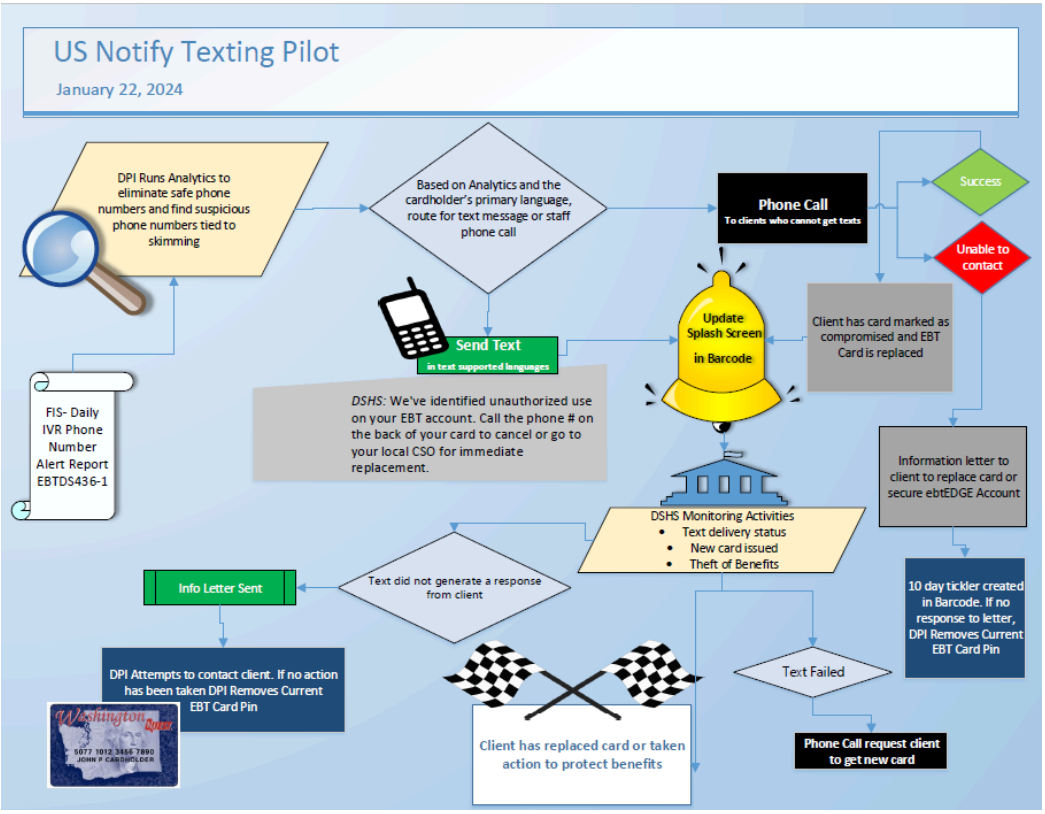
Planned outreach

When launching anything new, we knew it was important to prime audiences and support staff, but outreach takes resources and cross-departmental coordination. Given the large impact of fraud on customers and staff, DSHS was eager to start sending texts, so it prioritized no-cost, easy-to-run outreach methods before and through the texting campaign:

- Internal outreach, with staff notifications being sent statewide.
- A case management "splash" screen: DSHS used an internal setting for its case management screen that would send a pop-up to alert case worker staff if a customer's account was flagged with suspicious activity.
- Text messages sent to customers once analysis was completed that determined the EBT card may have been compromised. The text message advised the customers to safeguard their account by replacing the card, changing the PIN, or reporting the card as compromised.

- Social media: On Facebook, X (formerly Twitter) and Instagram, Washington created social media posts that included the phone number from which texts would come
- Development of an EBT Skimming flyer and Notify Text Message posters available in nine different primary languages.

Sent and tracked messages



The final steps of preparing for the outreach campaign included:

- **Developed indicators of success** to help the team track what a successful texting campaign would look like. Indicators included:
    - An increase in cardholders who change their PIN or freeze their account before funds are stolen.
    - An increase in the number of cardholders who request a new card before funds are stolen.
    - A decrease in the amount of funds stolen by criminal actors.
    - A reduction of manual staff outreach efforts.

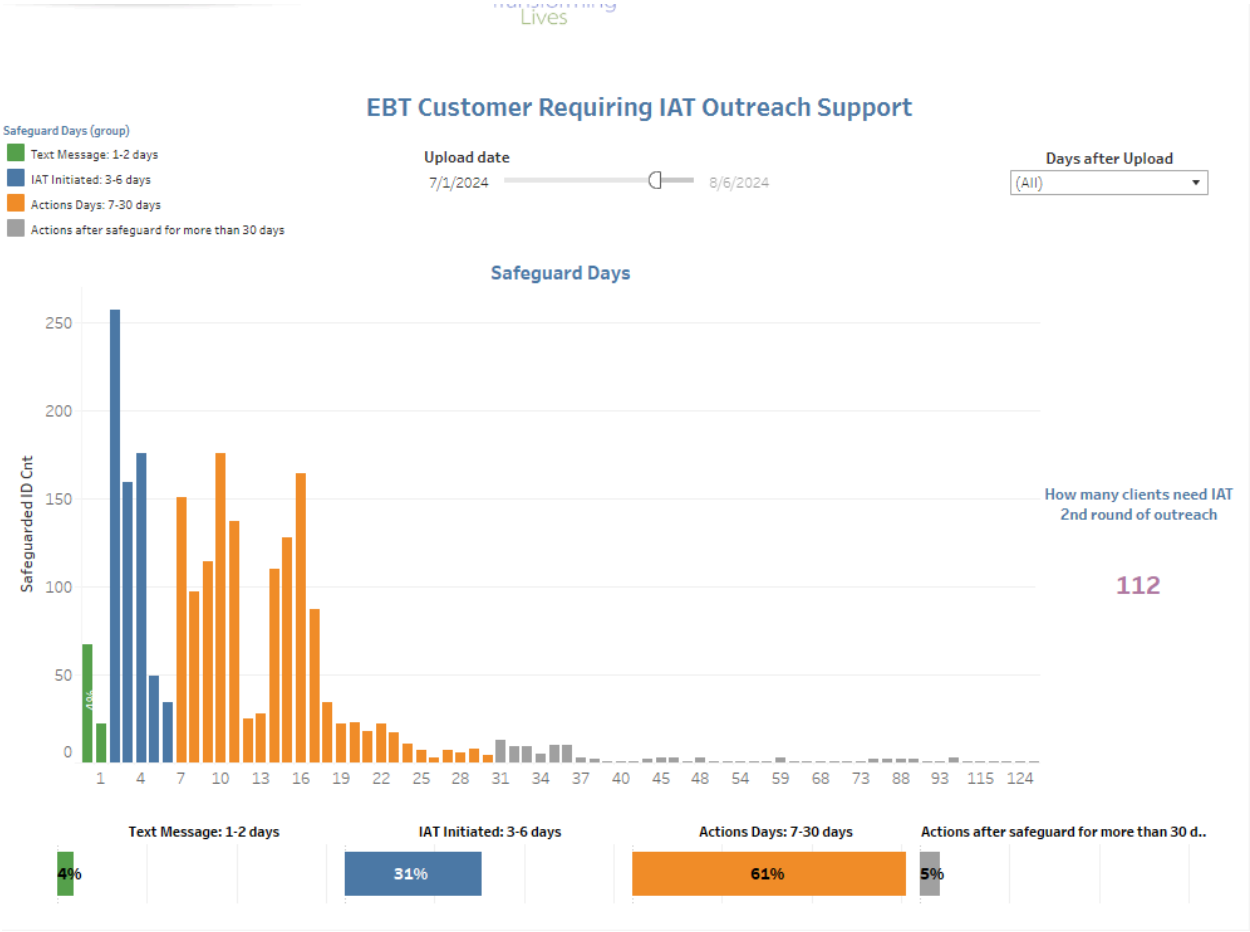
- **Built a dashboard:** From there, the team looked at internal systems for data sources and proxies in the system and created a visual dashboard in Tableau to help monitor these indicators.

    - This dashboard imported Notify.gov delivery information against client actions taken in the system.

- **Prepared recipient lists:** To send a text message with Notify.gov, a government entity needs a CSV or Excel file of target phone numbers.
    - To gather the customer phone numbers, Washington developed internal monitoring and analytic processes for revealing cards at risk.
    - Sending campaign messages in multiple languages required staff to create a recipient list for each language.

- **Developed a sending process:**
    - To support a proactive prevention approach, WA State determined that sending text messages daily would be most beneficial.
    - It was also determined the need to monitor safeguarding actions taken by the customers and assign a team to conduct follow-up outreach if customers don't take safeguarding actions on their own.

Lessons from piloting



Make impact tracking visible

- Washington started with a firm hypothesis and clear vision for what success would look like. Its visual dashboard, together with biweekly status meetings, helped keep an honest view of pilot success and put iteration in the forefront.

Leverage your entire communications ecosystem.

- No single outreach mechanism is perfect. Texting shows clear benefits in preserving access, preventing theft, and avoiding administrative costs, but thus far, only a minority of recipients (around 4%) have taken action based on text messages.
- In Washington, approximately half of the identified cardholders were initially reached by phone and took safeguarding measures based on that phone outreach.

In contrast, the remaining half did not act until after DSHS reset their PINs and a notification was mailed.
- Washington is working to get that texting percentage up and its staff outreach effort down, but some people will always respond better to a phone call.

Build trust before it's needed.

- We are conditioned not to trust unexpected texts or phone calls.
- The slow uptake of the first messages sent during the pilot period reinforced the importance of holistic outreach *before* that first text is sent.
    - Accessing some touch points was harder to achieve before the start of this campaign, and Washington still has the opportunity to keep building customers' assurance of DSHS's use of text messaging.
    - Additional Customer Communication Sources:
        - DSHS has its skimming approach online and is looking into adding specific language about the texting effort, including from which phone number customers can expect the texts to come.
        - It's adding a call center hold message about the texting program to increase awareness.
        - It's leveraging grant opportunities to get more printed and paid outreach resources.
    - Staff awareness is key to building trust. So far, however, some staff members are unaware of this effort or know the phone number from which texts arrive. Also, there are times when system alerts are not being viewed and/or used as expected
        - DSHS created flyers for local offices and sent them to community partners.

- Information was reinforced at staff trainings and meetings, where Division of Program Integrity was invited to present the pilot.

Change and add new content as you go.

- **Follow-up outreach to collect real-time feedback**
  - EBT cardholders were asked if they received the message and what they thought. Thanks to this qualitative feedback, Washington can pivot its approach in big and small ways.
  - Because impact tracking was at the forefront, DSHS got early feedback on messages that were thought to be untrustworthy.

Message	Iteration Rationale
Washington DSHS: Food or cash EBT cardholder, your benefits are at risk for theft. Please call the phone number on the back of your card or go to your local DSHS office for immediate replacement.	Add familiar terms about the benefits in question. In plain language, “unauthorized usage” turned into “risk of theft.” DSHS removed abbreviations and other confusing terms. For example, it changed “CSO” to “local DSHS office.”

- **Manage multiple language translations and iterations**
- **Use impact tracking to drive iteration**
    - Measuring impact and collecting feedback gave Washington foundational insights about how to expand its texting program.
        - WA State is currently developing a new “trust-building message pilot" that will send messages to communities most at risk for fraud.

The outcomes so far

- For recipients: Thus far, over 10,000 EBT cardholders have been texted, with over 9,000 individual benefits safeguarded.
    - Some individuals have experienced a loss in benefits because they did not act in time.
    - In some instances where the card PINs were reset, the customers utilized the same PIN and;
    - In other cases, criminal actors skimmed their EBT cards again
- For Washington State:
    - Added new campaign use cases to notify. Building on the success of the anti-skimming campaign, it used Notify.gov to remind people about SNAPQC interview appointments.
    - Approximately 300 EBT cardholders took safeguarding actions after receiving a text.
        - This decreased the need for Washington staff to call or take manual action on these cases. We've been told these phone calls can be time-consuming, ranging from five to 30 minutes, so these 300 safeguarding actions saved a minimum of 25 hours of staff time.

        - The hope is to eliminate the need to process stolen benefit claims, but EBT card skimming remains a national issue. The initial cost avoidance figures for customers safeguarded due to using the text message is approximately $135,000, but using this in conjunction with all other security safeguard outreach efforts is exponentially larger.

- For US General Services Administration Notify.gov
    - The nuances of using Notify.gov in real time helped improve that product.
        - Application Programming Interface (API) could help streamline processes, starting with automating delivery statuses and progressing toward sending messages.
- For USDA FNS
    - Since the approximately 300 EBT cardholders who took safeguarding actions after receiving a text helped prevent the theft of their benefits, they also helped USDA FNS avoid paying for these benefits twice via reimbursements to Washington. (Source: fns.usa.gov)