MIRS
Michigan's Independent Source of News & Information

NAME

House Oversight on State and Local Public Assistance Programs - 7 24 2025

DATE

July 25, 2025

DURATION

1h 23m

14 SPEAKERS

Chair Jason Woolford (R)
Clerk
Doug Woodard
Rep. Penelope Tsernoglou (D)
Rep. William Bruck (R)
Andrew Kustowski
Jennifer Allen
Rep. Steve Carra (R)
Chair Woolford
Rep. Denise Mentzer (D)
Jamie Topolski
Chris Carter
Alex Reilly
Rep. Ron Robinson (R)

START OF TRANSCRIPT

[00:08:29] Chair Jason Woolford (R)
Good morning. The Oversight Committee on State and Local Public Assistance Programs will come to order. If you'd like to testify on an item today or on an agenda on the agenda, please fill out a testimony card and turn it into the sergeant. Uh, will the clerk please call roll for today's attendance.

[00:08:49] Clerk
Chair Woolford here. Representative Bruck. Present. Carra here. Tsernoglou here. Mentzer here. Mr. Chair, you have five members present. You do have a quorum.

[00:08:59] Chair Jason Woolford (R)
Thank you. Uh, Representative Mentzer moves to adopt the minutes of June 12th, 2025 meeting. Uh, there being no objections, the motion prevails by unanimous consent. Uh, before we get started, I wanted to just read a quick statement that I wrote, uh, just very simply, as a husband, a veteran, a taxpayer, a. Father to, uh, children and and caring for people in the state of Michigan as a whole. Uh, I'm committed to stop, uh, the fraud in Michigan and, uh, specifically the fraud that's happening with these Michigan bridge cards. Hard-working men and women and trust all of us in this room with their taxes. With the money that they're paying in taxes, and expecting those funds to help people in need, not going to those that are fraud in the system or those that are stealing from it. So we must close these gaps. Hold these fraudsters accountable and ensure the Department of Health and Human Services continues to help stop the waste, fraud and abuse so that for every dollar that is going into these programs actually goes to supporting the people who are actually in need and then protecting those that use it. Thank you. Uh, first today we'll be hearing a presentation from the office of the Inspector General. After after that, we'll be hearing a presentation from conduit. And finally, we'll be hearing testimony from Representative Ron Robinson. Uh, with that said, I'd like to welcome, uh, Doug Woodard from the office of Inspector General. And please begin when you're ready. Good to see him.

[00:10:42] Doug Woodard
Thank you. Uh. Thank you, chair. And, good morning to everybody here. And on behalf of Stacie Sampson, our inspector general, I've got with me here today, Andrew Kustowski, the director of our Special Investigations Division, and Jennifer Allen, who's the manager of our Benefit Trafficking Investigation section.

[00:11:02] Rep. Penelope Tsernoglou (D)
Chair, I apologize, may I make a point of order before the presentation?

[00:11:05] Chair Jason Woolford (R)
Yes.

[00:11:06] Rep. Penelope Tsernoglou (D)
Um, just to be clear, the notice mentions HB 4515 that is not currently before this committee, but rather currently in the Government Operations Committee. I just wanted to ensure that our chair asks our guests not to discuss the merits of this bill or any other bill, which is improper, but to keep their comments to the general issue of bridge cards and their security, which it looks like this presentation is doing. But just wanted to clarify that with the chair and with our guests.

[00:11:41] Chair Jason Woolford (R)
Thank you. I appreciate your time on that. But 4515 is not being laid out before this committee. Uh, we're not considering this bill at all. Uh, today in this committee, the business before this committee is a presentation and a testimony on the topic that coincides with the policy bill and other committee, which is in another committee. Uh, this oversight committee is engaging in its duty to gather information and possibly provide policy recommendations to other committees, which within the scope of this committee is. So no motions regarding 4515 will be considered today. Thank you. Go ahead.

[00:12:18] Rep. Penelope Tsernoglou (D)
Chair, appeal the decision.

[00:12:21] Chair Jason Woolford (R)
We'll go at ease.

[00:18:21] Chair Jason Woolford (R)
The committee will come back to order. Representative Bruck.

[00:18:26] Rep. William Bruck (R)
I moved to table the motion without objection.

[00:18:29] Chair Jason Woolford (R)
So ordered. Uh, the clerk will call the roll. Oh, no. We're good. Okay. All right, so we're good to go. Thank you. Uh. Go ahead.

[00:18:42] Doug Woodard
Okay. It says, as I said earlier, uh, I've got, uh, Andrew Kustowski and Jennifer Allen with me. They're working our teams. Uh, Andrew's the director of our special Investigations division, and Jennifer is the manager of our Benefit trafficking investigations section, which does a lot of the work, is involved in a lot of the work today that we, uh, we're going to be talking about. Presently, Michigan, along with 48 other states, operate their food programs with magnetic stripe technology. This year, California was the first state to utilize chip technology, and others are moving toward in that direction. Over the past three years, Michigan has averaged nearly 1.4 million fat recipients and 250 million in fat benefits paid out monthly Each of these recipients represents a potential conduit for bad actors to steal fat benefits through skimmed EBT cards. Shipping the bridge card will help reduce stolen benefits. Within the past few years, criminals have utilized skimmers or shimmers at point of sale devices to copy and produce counterfeit cards. This image shows how small the components are to produce a shimmer, which is on the top, and a skimmer, which is on the bottom left, and 100 pack of blank EBT cards costing $41.87 from a well-known office supply company. Once a recipient's EBT card is compromised, criminals can then access EBT benefits for as low as $0.41 per card. This is a photo of the common components used to build a card skimmer. These items are easily purchased on the internet through legitimate businesses, typically for less than $10 each.

[00:20:39] Doug Woodard
The items pictured here are currently for sale through Amazon. Bridge cards updated with chip technology would require bad actors to intercept the current digital code, and then enter the Pin while the card is still processing in the point of sale terminal to complete a subsequent transaction. Tap to pay on enabled chip cards is even better at preventing fraud by tokenizing the transaction instead of transmitting card details. Tap to pay sends a one time use code. This method reduces the risk of encountering a skimmer or shimmer, as there is no physical contact with a point of sale terminal. Now we're going to talk a little bit about what we're doing to combat stolen benefits. This is a photo of a skimmer attached to a card reader of a store. This past year, MDH OIG developed algorithms and analytical tools for every detection for early detection of compromised accounts and skimmer locations. Our EBT skimmer analysis uses geolocation data and recipient shopping patterns to identify potential placement of skimmers at retail stores. Oig partners with USDA OIG when we identify skimmers. These analytic activities have resulted in the detection and confiscation of 44 skimmers at Michigan retailers, and have safeguarded over 76,000 individual bridge card accounts and more than $16.6 million in food stamp funds. Our OIG continues to locate point of sale terminals utilized to steal FAP benefits. Oig has identified over 300 terminals at unauthorized locations using the terminal IDs of an FNS authorized location to process payments.

[00:22:48] Doug Woodard
OIG requests a Pin reset, which requires the recipient to reset their Pin before using their bridge card, as their old Pin was potentially compromised at the store when utilizing a cloned point of sale device. A search warrant was executed by local law enforcement and Jennifer's team at one of these unauthorized locations, and evidence of fraudulent FAP transactions and other financial crimes were located and seized, including several electronic card readers, as seen here. These card readers are believed to have processed hundreds of thousands of dollars in fraudulent EBT transactions. Oig recovered these bridge cards and several others from an unauthorized retail location that was completing illegitimate benefit transactions. Earlier this year, we sent a recommendation letter to the Secretary of the US Department of Agriculture. Through our investigations, we found that third party processors do not have a method or ability to verify the FNS number that is used by merchant applicants for terminal setups, which allows the criminal groups to deceive these processors by providing false information about their businesses. The veil creates a lucrative method for these bad actors to easily conduct and conceal EBT fraud at the terminal level. These are IG's Org's efforts and outcomes from last year. Our efforts to reduce fraud, waste and abuse ensure that taxpayers money is spent on its intended purpose and benefit programs are operating as expected.

[00:24:43] Chair Jason Woolford (R)
Thank you. Thank you for your testimony today. Thank you for the hard work that you and your team are doing, and the amounts of money that you're helping taxpayers, those that are working, sometimes two jobs to provide benefits to those that are in need. But then seeing the fraud and and the thievery. So thank you for doing a good job on that I appreciate it. I do have a few questions for you today. Uh, I know the last time that you were here, uh, we were talking on a few different topics, but we're actually talking about the actual card itself today. So you mentioned converting bridge cards to chip cards and possible, um, bid that you were already looking into at our last hearing, which is why we asked you back again today. And additionally, uh, uh, having, uh, a company come in to testify today regarding that as well. Uh, so with this conversion of bridge cards, uh, fall into the category of fraud detection or, uh, prevention or both.

[00:26:07] Doug Woodard
It would be fraud prevention for sure. Uh, depending on the vendor and what we would set up in the contract, there could be some detection as well.

[00:26:17] Chair Jason Woolford (R)
Okay. And, uh, do you have. And if you don't, it's okay. But do you have an estimate or have you done any calculations to determine how much fraud this conversion could possibly prevent? When we're seeing the amounts of fraud that you've found in the amounts, but now having additional pieces, uh.

[00:26:42] Doug Woodard
We don't have an accurate number that we can give you or even estimate on. Um, Jennifer's unit works on this, uh, on these cases all the time and works with other law enforcement authorities. Uh, it is a problem, but I can't tell you what the actual number is.

[00:27:00] Chair Jason Woolford (R)
Sure. And on the previous slide, was it, um, what was the amount in millions that you were able to to save or find?

[00:27:09] Doug Woodard
Uh, we had a $305 million impact through fraud detection, avoidance and disqualifications last year. Okay. That number has been trending up over the years. Uh, in all the programs, not just food assistance.

[00:27:21] Chair Jason Woolford (R)
Great. So it would probably be safe to say if that we've we've found hundreds of millions of dollars. Right. Um, and that, uh, we might be able to find even more with more safeguards and, uh, uh. Things to stop us. Correct.

[00:27:42] Doug Woodard
I would say, yeah, we we we can prevent more. Uh, would be probably even better. Um, the pay and Chase model of investigative agencies like ours is it's really, actually better served to prevent fraud from happening than than chasing the money. Especially since, uh, it goes all over the all over the map.

[00:28:07] Chair Jason Woolford (R)
Thank you. Uh, what, uh, type of fraudsters have you identified in your work that would, uh, steal or use someone else's, uh, Bridge card?

[00:28:22] Andrew Kustowski
Typically in this scenario, what we're seeing is organized crime. You know, and it's not the traditional organized crime that you see in the movies. It's groups of individuals that have a propensity for knowledge on computer systems and how to build or EBT card skimmers that work together and create opportunities for them to steal benefits from the department.

[00:28:47] Chair Jason Woolford (R)
Okay. And let's talk just a little bit about that impact. How often do do these fraudsters use someone else's bridge card. And then also uh, have you seen, uh, the same name from the same people with cards, uh, with fraud? I know that's a two parter, so I'll repeat it.

[00:29:14] Andrew Kustowski
As you know, we've testified in the past. We only know about the fraud that we detect. Um, with that in mind. You know, Jennifer and her team, um, they interact at the recipient level with the people and the names, and would probably be better able to answer that question for you.

[00:29:33] Jennifer Allen
Yeah. So we do have some cases that are, um, ongoing that we've identified that it is the same individuals or same group of individuals that are involved in these.

[00:29:43] Chair Jason Woolford (R)
Mhm. And then what is done with that information. And what have you seen as follow up and follow through.

[00:29:50] Jennifer Allen
We investigate the case and we prepare it for prosecution.

[00:29:53] Chair Jason Woolford (R)
Okay. Wonderful. Thank you. Appreciate that. Is it, uh, easy to identify those who commit, uh, to being to this organized crime and and putting a stop to it, or is it something that you, you feel is just so big that it's it's hard to wrap your arms around.

[00:30:21] Doug Woodard
We have a robust internal analytics unit within our department, within our agency that does an awesome job in detecting any new trends. And I think I previously previously said that the trends don't stay the same. It's a moving target and that's what makes it more difficult. We're here talking about chip card technology. Today while we're a mobile wallet is now becoming a trending new new way to pay. So part of the frustration is, is government is generally 10 to 15 years behind the banking sector. So we we follow along on a slower trail. And I'm not blaming the state governments, the federal government in this case, it waited till late late last year and in between November and December to let the states know that they were authorized to do chip cards, and they are testing mobile wallet technology. So to answer your question, uh, there is some frustration in, in trying to in getting your hand wrapped around what's coming next because there's always a new trend of of and there's oh, whenever somebody says to me, well that'll prevent fraud. Yeah it will until and it slows it down for sure. But there's always new technology being developed by fraudsters and people. And that's why we have companies like antivirus software that constantly have to stay ahead of the game.

[00:31:49] Chair Jason Woolford (R)
Awesome. Thank you. Uh, I will note that I had the privilege of going to the white House a few weeks ago and meeting with the president's cabinet, and I was able to have a one on one, uh, or a one on one conversation with the, uh, the secretary, uh, Kennedy. And he had shared, uh, when we were sharing some of the information from here in Michigan. We have his number one contact and said that he wants to work with the state of Michigan and us to to stop this waste, fraud and abuse. So I'm excited about the continuing of that relationship because that will help give you some help as well on your team, given your, uh, well, I guess before I get to that, how might converting bridge cards to chip cards help in your fight against this organized crime and from individuals? Uh.

[00:32:44] Doug Woodard
I would say that, uh, we've got newer actors coming in the game that, uh, can purchase, like we showed in the presentation, things for pretty cheap to, to to rig up a skimmer, uh, for them to, to, to get beyond chip technology is going to take a while. Uh, some of them will get to it quicker than others. But the reality is, is as they advance, we have to we have to block those measures. And, um, as stated previously in that in our presentation, the swipe card technology is so easy to copy. There's no, uh. Uh, you, you and I can go out and buy a card reader tomorrow and read any amount of information that comes on a, on a, on a swiped card. So just that that in itself is going to stop some of this.

[00:33:35] Chair Jason Woolford (R)
Mhm. That's great. And uh you know I'm glad to hear you speak in those terms of speaking on the importance of that. Anything uh helps. Uh, right. Uh, I think about, uh, I was in the Walmart, uh, a month ago and, uh, it might have been two months ago. And there was a young girl who was there with her two babies, and she told me that she works two jobs. And she was talking about, uh, the cost of eggs and, uh, how she couldn't afford them and that she was going to have to go buy, uh, you know, something other than that to not being able to give her kids a proper, healthy breakfast. The reason I say that is she's working two jobs. Uh, being taxed over taxed. Uh, and, uh, um, it's important for those people that are working like that to know that the money that they're paying into the system and taxes are doing anything and everything they can. And while there's no silver bullet, so to speak, in this, uh, putting some of these safeguards into place, uh, chips and pictures on cards and the things not one of them is an overall fix, but they will continue to stop some of this fraud. So thank you for that. Uh, just once. Uh, Representative Carra.

[00:35:01] Rep. Steve Carra (R)
Thank you, Mister Chair. And thank you for your testimony. You you mentioned earlier that there was over $305 million in fraud, cost avoidance and disqualifications that you were able to detect, and there's fraud that you were not able to detect. Do you have any ballpark estimate on how much total fraud you believe that there there was?

[00:35:21] Doug Woodard
No we don't.

[00:35:23] Rep. Steve Carra (R)
It's certainly more than that. And you did the best you could.

[00:35:25] Doug Woodard
We did the best we could. We find whatever fraud we can. Right. And we we we we aggressively go after it. Uh.

[00:35:33] Rep. Steve Carra (R)
Right. And if we can prevent it in the first place, the argument would be that'd be better than chasing down the fraud after it occurs.

[00:35:39] Doug Woodard
It's always better to to prevent.

[00:35:41] Rep. Steve Carra (R)
Okay. Thank you.

[00:35:45] Chair Woolford
Representative Mentzer.

[00:35:47] Rep. Denise Mentzer (D)
Thank you, Chair. And if you don't mind, I have two questions. Sure. Um, a good part of the fraud seems to come from retailers who take those cards and cash them out. Um, what kind of penalties? Sanctions. Fines? Uh, punitive action. Uh, do you take against these these retailers that cash these cards out?

[00:36:11] Doug Woodard
Good question. The retailers are handled by USDA OIG. And they're the the investigative body that handles, uh, retailers. We are not in the full scale retailer business. So we don't have the penalties and sanctions that they they impose on their retailers when they're found, but they generally will lose their ability to sell, uh, and utilize bridge cards in their facility. They will shut them down. Uh, and they also look to prosecute the, the, uh, stores as well. It's pretty high threshold though.

[00:36:47] Rep. Denise Mentzer (D)
Okay. And one of the other things I was a little concerned with here in the our legislative analysis, it talks about federal regulations and that retailers are not allowed to prohibit individuals who have an EBT card in a valid Pin from using the card if they are not pictured on the card and it says. Therefore, individuals with a bridge card and a valid Pin will be able to use the card regardless of whether or not the photo on the card matches. So is there any effort or, you know, maybe something chair that you spoke with Secretary Kennedy about about changing the federal regulations. Because if if federal regulations say you have to take that card whether the picture matches or not. Um, that seems to me very problematic.

[00:37:36] Chair Jason Woolford (R)
Absolutely. That that specifically was some of the exact, uh, stuff that we were, were talking about. So. Thank you.

[00:37:44] Rep. Denise Mentzer (D)
Yeah. Do you have any comment on that?

[00:37:49] Doug Woodard
Uh, comment on the on the the federal regulations? Correct. That. Yeah, that you're correct in that federal regulation. I've got a few of the federal regulations in front of me, and there is, uh, the retailer cannot stop them and anybody can hand somebody else their bridge card, uh, to use to, to purchase for them. Their name doesn't have to be on the card and their face doesn't have to be on the card. So there's really, uh. Uh, we get police officers that call us all the time, that call our agency and say, hey, somebody was stopped with somebody else's bridge card. Um, and if it's one bridge card and they say they were shopping for the family, it's totally okay. But if it's 25 bridge cards and they appear to be involved in something nefarious, then that's something we we definitely look into. So it depends. You do have people who are shopping for a foster home or something where they might have multiple cards, and that might be totally legit, but it's something that we, we look at. Uh, but that has to do really with matching names. Not necessarily with photos.

[00:38:56] Rep. Denise Mentzer (D)
Thank you.

[00:39:02] Chair Jason Woolford (R)
Well, uh, unless anyone has any other questions, which it doesn't look like we do. I thank you for your time today. To you and your team. And we'll continue. I can promise you, we'll continue working to to bring some clarity. And just as it related to the pictures. Um, we know that regardless of that process, uh, having people to potentially come in and have to get their picture and that user on that card, I don't know how many organized crime members and people that are thieves will want to come in and get their picture on someone else's card. Thank you for being here today. Appreciate you.

[00:39:52] Chair Jason Woolford (R)
At this time, I'd like to welcome, uh, the team from Conduent. And, uh, please come when you're ready.

[00:40:14] Jamie Topolski
Hello, my name is Jamie Topolski. I'm the director of government payment products for Conduent.

[00:40:20] Chair Jason Woolford (R)
I'm just real quick before you get started. Thank you for being here today. Uh, and thank you for for being here and being, uh, able to present on an idea of converting bridge cards to chip cards. Uh, in the spirit of transparency, I would like to state that it's my understanding that you've already have a bid in with the OIG to possibly complete this conversion, and this is something that you've already been potentially working with with the state of Michigan.

[00:40:51] Jamie Topolski
Um, we work with several states on this initiative. I do not believe we currently are working with the state of Michigan on this initiative. Uh, the state may be working with a different vendor at this time. We're here really in the informational, in the capacity of information sharing.

[00:41:06] Chair Jason Woolford (R)
Great. Thank you. Uh, go ahead when you're ready.

[00:41:10] Jamie Topolski
Terrific. And then I'm fortunate also to have two colleagues join remotely. Uh, via zoom. Um, if they want to introduce, we have, uh, Chris Carter. Chris, do you want to introduce yourself if you're able to.

[00:41:22] Chris Carter
Yeah. Glad to thank you, Jamie. Thank you. Committee. My name is Chris Carter. I'm the head of fraud for the public sector. Uh, work closely with with Jamie and, uh, specifically on EBT, um, cards. So looking forward to the conversation and seeing how we can work together on this.

[00:41:38] Jamie Topolski
Thank you. And, Alex, do you want to introduce yourself as well?

[00:41:41] Alex Reilly
Yeah. Thank you Jamie. Great to meet you. Committee. So yes, my name is Alex Reilly. I'm a fraud expert of about a decade of different fraud experiences. So really pleasure to have you. As I focus on EBT and some of our also open loop programs. So those are in the way to go programs. So pleasure. Thank you for having us.

[00:41:57] Jamie Topolski
Great. And I may turn to them to answer some questions and to fill in some gaps as well. But it's great to have them joining us as well. So we're going to cover a couple of topics. I just want to go at a high level, understand the current landscape of fraud, why we're some of the reasons why we're in these difficult situations right now. Some of the current industry standard fraud tools that are available that can help address they may not be leveraged fully, but they are available now and then. Some of the cutting edge future technologies that can help with this problem as well. So those three types of topics we'll be discussing. So let's talk a bit about the current fraud landscape and some of the challenges that we see. Um, it's helpful to consider the differences between the cards that we have in our wallets, our credit cards and debit cards, and the bridge card, because that really points to some of the challenges that we are up against. So there with your credit cards and debit cards right there branded Visa or Mastercard, Discover or American Express. And those organizations set all sorts of rules and technology controls and provide consumer rights for how they can use that card and protections for the consumers. And there aren't comparable controls and governing agencies similar to those private companies.

[00:43:17] Jamie Topolski
To protect the bridge card, bridge card infrastructure and the recipients of those benefits. So, for example, if someone manages to steal your credit card or debit card and use it, you as an individual are protected against that type of fraud. The money will be restored to your account in most cases, unless you are negligent in notifying your your bank or credit union that your card has been stolen. There is no comparable protection for benefit recipients and no oversight to protect against that. There's no ability to easily charge back or dispute transactions on on the bridge card. In most cases, it's much more complex to do so than to do so with a credit or debit card. Um, and there are some regulatory gaps as was discussed. Sometimes the retailer is unable to decline a card that they might feel, uh, isn't properly being used, or the processor might not be able to decline the transaction because the rules say that the transaction must go through the card must be accepted. So there's a bit of, uh, inflexibility in enforcing certain types of controls that might help reduce fraud. In terms of the technology, as the OIG, um, presentation showed. So, um, really clearly the cards are leveraging very old magnetic stripe technology. There are 100% correct. Anyone in this room could purchase a device to read the magnetic stripe off of any card, and to write it onto any other card very, very easily.

[00:44:45] Jamie Topolski
With any laptop computer you plug it in, you install all over the software and it works by itself seamlessly. Very, very easy. And the criminals know this. They're able to get the data off of cards using these skimmer devices. But what's interesting is these skimmer devices that are installed on the point of sale terminals, they're still stealing the data in many cases of our chip cards. The difference is that you can't use stolen chip data to make a fake card. Because, as the OIG presentation rightly pointed out, there's a unique code for every single transaction. So the criminals can still get their hands on the data. They just can't use it to make a fake card. They can't make a fake mag stripe card, and they can't make a fake a fake chip card. So even though they still have the ability to get their hands on the information, it's useless to them. They can't shop online with it either in most cases. So it's really an extremely, extremely effective technology. And even though the underlying technology is quite old, and in fact it's been used since the late 1990s in Europe and Asia, the keys and the cryptography that go into these chip cards continue to get stronger and stronger so that the criminals can't, you know, crack the code to crack the keys.

[00:45:58] Jamie Topolski
So it's really a very, very effective way to counteract counterfeit card fraud and skimming problems. The OIG also talked about some of the issues with point of sale terminals that criminals are getting their hands on terminals using incorrect or loading them with FNS numbers that they are not entitled to load. The processors of those transactions don't know that that these are illegitimate uses of the FNS number, and lots of transactions are getting used to get fraudulent money to remove money from the cards fraudulently so they get their hands on the fraudulent cards, they have a fraudulent terminal, and they just work their way through them very, very quickly. So you see that as well in the terminal, the attacks against terminals. And then they also the criminals are also using the telephone systems to commit fraud. So they're calling into the IVR for the bridge cards, the numbers on the back of the cards and attempting to figure out how much money is on the card. What's the pin for the card? They will attack day after day. And if we determine that the card is a phone number that they're calling from is fraudulent, will block that number, but they have the technology to move to another number very, very quickly.

[00:47:08] Jamie Topolski
So they're attacking really multiple channels. They're attacking the card by skimming and cloning it. They're attacking the point of sale terminals and the merchants by illegitimately using FNS numbers on fraudulent terminals. And they're attacking the back end telephone systems and data systems to try and get data that's useful to help them commit the fraud. And these are the sorts of things we need to think about when we try to come up with solutions. So what are some of the standard tools that are available today? Some of these are going to seem almost, um, you know, laughable in terms of how simple they are. But but believe it or not, these still need to be implemented in some cases, just enforcement of using a secure pin, right? Don't let someone use one, two, three 4 or 1 111. We keep reading stories. Um, you know that people use passwords for their secure systems. Use the word password or something. Or their name. Right? It's the same sort of thing with a Pin if you use an easily accessible pin. Uh, it makes it that much easier for the criminal who steals your card or steals your data to guess the pin very, very quickly without having to try, um, 10,000 possible combinations.

[00:48:16] Chair Jason Woolford (R)
So you're saying if my code's 111, I should probably change that today? Yes.

[00:48:21] Jamie Topolski
Okay, a good idea.

[00:48:22] Chair Jason Woolford (R)
Um, it's.

[00:48:23] Jamie Topolski
And it's amazing how common those standard, you know, 43211234. And so we have, uh, controls in our systems to prevent if someone has more than two consecutive numbers that are the same or numbers that go in order, you know, upwards or downwards for more than three digits. We'll reject that pin and ask them to select a more secure pin. It's it seems basic, but it does help. Um, notifications. Right. Uh, getting a text message or an email. Whenever you have a transaction gives you the opportunity to say, hey, that I wasn't at that store. I didn't make that purchase. And then in combination with the third item listed, then being able to lock your card. The card lock is something that could be more highly leveraged by the by bridge card recipients and other card recipients. The challenge, of course, is that it requires proactive measures by the individual. You have to go in and lock your card and unlock it when you want to use it. But ultimately, when your card is locked, it does prevent a criminal from emptying the account. So it is a nice feature to have. Um, doing a pin reset whenever someone receives a new card in the mail or in person, having them reset their pin, having them authenticate so a criminal could intercept a piece of mail and get that card.

[00:49:44] Jamie Topolski
And if they just have to enter the information that's on the card, they have everything right there in front of them. It's very, very easy. But if you also ask what's your date of birth? What's your case number for your EBT benefits? You know, things that the criminal wouldn't know. What's your Social Security number? The criminal who has stolen the piece of mail doesn't know that additional piece of information, so they can't complete the card authentication process, can't use the card. It's another nice feature that can help reduce the amount of fraud. We talked about how criminals are attacking the phone systems. Having more robust systems, detecting fraud on our phone systems can help as well. So, for example, being able to score the likelihood that a call is fraudulent because we've seen that number used with multiple card accounts or card numbers. That's a way to block cards, calls that are coming in from criminals who are trying to get data about a stack of cards that they've stolen, and then, of course, transitioning to EMV chip cards. We'll talk. I'm going to talk a bit more about the EMV cards. So what the EMV cards do?

[00:50:55] Chair Jason Woolford (R)
Excuse me. We have a couple of questions specifically on where we're at in the PowerPoint. Uh, Representative Carra.

[00:51:03] Rep. Steve Carra (R)
Well, thank you, Mr. Chair. And thank you for your testimony. I guess my question would be if we do switch to the chip cards, would we have a magnetic strip and a chip card on the same card, or would it exclusively just have the chip card?

[00:51:16] Jamie Topolski
So you would need to have the magnetic strip on the card for the foreseeable future, because it would take several years for all of the retailers to switch over. And also, um, there are ATMs where you insert your card into, there's a little door that opens, and the presence of the magnetic stripe actually is what opens that little door and lets the card get sucked in. So even even if you don't need it for retailers, you still need that magnetic stripe in most cases to in certain types of ATMs.

[00:51:50] Rep. Steve Carra (R)
And in the case where you have to use that magnetic strip to open the door, basically, would that be enough to where it could be skimmed, or would that not have enough of the strip to be skimmed in that circumstance?

[00:52:01] Jamie Topolski
Well, you could do there's two approaches. You could say the magnetic strip is there, but there's no meaningful data on it. Um, the way we handle that traditionally in the chip world is the the data that's on the magnetic strip is different than the data that's on the chip. So again, if someone steals the data off the magnetic strip, you can't use it to make the fake chip. And in fact, what you can do is say, okay, if we know that the if we know that the retailer is supporting that chip and we know that the person has a chip card in hand, decline the magnetic stripe transaction, don't allow it to go through. Force the individual to use the chip. If you take your debit or credit card and try and make a purchase at, you know, CVS, Walmart and the store. By swiping it, the terminal is going to say, please insert the chip. It's going to force you to use the chip. Only if you really try multiple times might to let go through, and then the bank may decline the transaction anyway. So there are back end systems where you can say, yeah, the magnetic stripe is still there. You can still use it at the retailer that doesn't yet support the new chip, but everywhere else that does. If someone swipes the card, declined the transaction, force them to use the chip that you spent good money to put into the card.

[00:53:14] Rep. Steve Carra (R)
Okay. Thank you.

[00:53:18] Chair Jason Woolford (R)
You can continue. Thank you.

[00:53:21] Jamie Topolski
So as I was mentioned by the OIG that it really the putting the presence of the chip really does cut down significantly on counterfeit card fraud. But the second thing we're going to do in conjunction with putting the chip in the card, is add a three digit security code to the back of the card. So again, we all shop online and we're used to being asked, what's the security When you check out, please enter the security code from the back of your cart. There isn't a single card bridge card that exists today that has that three digit security code on the back of it. Because until the pandemic, there was no online shopping for Snap benefits, so there was no need to put that security code. But now there is online shopping. And so to help prevent all the fraud from migrating to the online channels, you need to have a security code on the back of the card. It really is not directly related to EMV, but you kind of once you're reissuing the plastics, you put the chip in the front, you put the security code in the back, and you ask the online retailers to demand that security code as part of the shopping checkout process. And that way, when the criminal skims the magnetic stripe, they don't have that three digit code from the back of the card.

[00:54:33] Jamie Topolski
It doesn't exist anywhere on the card except printed on the back. So unless the criminal has that physical card in their hand, They can't shop online with that stolen data. So the chip on the front of the card prevents counterfeit. The three digit code on the back of the card prevents online fraud. So okay, then we talked that we do mention digital wallet. It's a much more complex technology to implement getting the cards into Apple Pay and Google Pay. It's tough to do. It also introduces a different type of risk that we need to be aware of. It's called provisioning risk. When you mail a card to someone's physical address, you know you know where the card is going. Hopefully that person still lives at that address. But when, um, when you receive a request to to what's called provision a card into someone's mobile phone to get the card into their Apple Pay or Google Pay, it's very, very challenging to know whose phone is this that I'm going to send this card into. Is it the is it the legitimate recipient of that bridge card benefit? Or is the criminal who was claiming to be that recipient? It takes a lot of effort and a lot of thought has to go into it. It's not insurmountable, but it's something just to be aware of the challenges.

[00:55:54] Chris Carter
In Jimmy Carter here. If I could jump in around the digital provisioning, there's also fraud strategies and traditional fraud environment that are deployed in the time while that card is in the mail, which you lose during the digital provisioning. So that just goes to speak to the strength of that provisioning process needs to be very robust, because now you're talking about giving a card to somebody in seconds versus 3 to 4 days, where typically you can detect account takeover and work to mitigate the bad guys before that card reaches them in their USPS mailbox. So a lot goes into that digital provisioning. The timing is great. It's convenient, it's helpful for everybody. But if not done properly, the fraudsters will exploit that and drain the cards within, you know, minutes versus a couple of days that it takes for a physical card to be mailed.

[00:56:38] Jamie Topolski
That's a that's a great point. Yeah. It sometimes faster isn't better when it comes to potential for fraud. So a question was asked earlier about can we estimate how much fraud could be reduced. And it's very tough. Every situation every card portfolio is different. But we do have some good data that visa published back um, in I think 2019 that showed how their migration to chip card from stripe was being effective in the US market. So what? This slide's a little busy, but it shows basically for retailers that had implemented support for Chip. Once there was, say, an adequate number of cards out in the field have been replaced. Counterfeit card fraud loss dropped by 87%. And this was before full penetration. So this is when, um, 80% of retailers had made the conversion and 72% of the plastics had been converted, so not even 100. Not all. Not all your bridge cards are done. 72% are done. You know, 80 out of 100 retailers have flipped. And the fraud dollars, counterfeit card fraud dollars fell by 87%. And I don't have updated data. They never published this again. I suspect it's only continued in that trajectory.

[00:57:59] Chair Jason Woolford (R)
So when did the, uh, private sector with credit cards. When did they start? What year did they start putting in chips in the card?

[00:58:12] Jamie Topolski
Yeah, the big rollout really Started in 2015. So what happened was I think it was late 2011, there was a very public breach of target's credit card system, followed by several other very prominent breaches. We all started. You don't remember? We all started getting replacement cards in the mail. Uh, you know, on a monthly basis, it seemed like there was a breach after breach. And so this is going from 2015 to basically over the course of three and a half years. This is the drop. It was a 87%.

[00:58:44] Chair Jason Woolford (R)
So that's fascinating to me. You look at the 87%. You look at nearly ten years that we, as the state of Michigan, uh, could have implemented something like that, uh, at the tune of the OIG testimony of around $300 million, which we know it's way more than that, but let's just say that's the number. Uh, we're talking about $4 billion of people's money that has been taxed, uh, and stolen or wasted. So, uh, I'm very excited to see that that slide on that 87% and only can imagine, uh, the billions that it will save over the next few years in the state of Michigan. Should this work?

[00:59:28] Jamie Topolski
Thank you. Yeah. And that would encourage the link. The sources there included the link. Uh, there is a whole PDF that visa did publish that might be helpful as well containing additional data.

[00:59:39] Chair Jason Woolford (R)
And you had mentioned also online shopping like Instacart and things like that. Uh, this would uh, uh, obviously stop a huge amount of that. And the percentage of people, uh, using Instacart and those online shopping is obviously increasing. Correct?

[00:59:58] Jamie Topolski
Yes. What happens is, yeah, the criminals, to the extent they can be, uh, will be lazy. And if it's easier just to empty all the cards by shopping online and having to physically go into a store where there may be on the security camera. Right. It's why not I get if I can steal from the comfort of my own home and couch with my laptop, I'll do so. Um, again, the the the the addition of the three digit security code to the back of the card. So right now, when you shop online with a bridge card, you do need to enter in your Pin. So there is some security there. But again, the criminals are. That's that skimming device that we saw in the OIG presentation. It was a complete overlay. So it gathers all the data from the magnetic stripe and it captures the pin. Because the pin pad is an overlay as well. That's how they know your card information and your Pin number. And then they can shop online or at any other store they need to shop at. They sometimes use cameras and they sometimes use the overlays.

[01:00:58] Jamie Topolski
And what's amazing is that it used to be a few years ago, the criminals had to go back and retrieve that to get the data off. No, they just installed little Bluetooth transmitters into those things now, and they just go within, you know, 20ft of it. So someone comes back in the store, it transmits all the data to their phone, and then they have everything. They don't have to touch that terminal ever again. They just go in periodically. It's unbelievable. But the addition of the three digit security. So now what you're talking about for online shopping is a four digit Pin and a three digit security code. So there's 10,000 possible pins. A thousand possible three digit security code. So the exponential combination right now the criminals are patient. They will cycle through those those pins. They'll try all the common ones and then they'll try some others. They will eventually get the right pin. But once you add to that, the three digit security code becomes exponentially. It would take them years to get the right combination that really isn't effective.

[01:01:55] Chair Jason Woolford (R)
Thank you. Representative Mentzer.

[01:01:59] Rep. Denise Mentzer (D)
Thank you. Chair. I have kind of a strange question when you consider, you know, most people would do their, you know, ate grocery shopping at, you know, like Kroger and and Walmart and, and Myers and it says here that 80% of retailers accept the chip cards. Where are people who have EBT cards? What is this other 20%? Is this the gas station grow, you know, a fast food store? I mean, what kind of stores are these? And and I guess I'm confused why there wouldn't be some kind of a limit that EBT cards could be used. Um, only in, in in certain types of stores.

[01:02:46] Jamie Topolski
Yeah. So this was, this was the statistic back in early 2019. So the percentage right. You're absolutely right. Now almost every retailer, it's hard to find a retailer where you can't use your chip card. Gas stations were one of the last to implement because, uh, the poor station owners, they had to change every pay at the pump terminal. I think about all the pumps and they had to swap out. It was a very lengthy and expensive process for them to to do that. Um, and the thing that's important right now is that all the retailers that can accept chip cards, they're going to have to make a small upgrade to the software to support the EBT chip card, because every every chip card, like a visa chip card versus a Mastercard discover. And now EBT has a slightly different code in it so that they can when you when you either tap or insert your chip, it knows, oh, this is a visa debit card. This is a discover credit card. This is a snap EBT bridge card. And it knows what the rules are for that card. So with a bridge card the terminal says, oh, it's a bridge card. I have to ask for the pin. Every single transaction. There's no way to make a snap purchase without entering my Pin. It enforces that. But with your credit card, most of the time it doesn't ask you for your Pin. It knows that by the code that's in the chip. So there are there is work to be done by the retailers, which is an important thing that we all need to keep in mind and push for. There needs to be, at some point, a deadline for every EBT accepting retailer to support this new chip standard. The the worst thing would be for the state to go through and go through all the costs of issuing these cards, and then the retailers not being able to leverage the technology of the chip, because then they haven't made that minor upgrade. So the two have to go hand in hand. The card issuance and the retailer support for the chip, both pieces must be.

[01:04:42] Chair Jason Woolford (R)
Thank you. Uh, and, uh, just so you know, we we have about, uh, 5 to 10 minutes left, so I know you have two slides left. So if we could get through those. And the most important parts of those. Thank you.

[01:04:53] Jamie Topolski
Yep. Sure. Sorry I'm being long winded, so.

[01:04:55] Chair Jason Woolford (R)
Oh, no. You're doing great. Thank you. Yeah.

[01:04:57] Jamie Topolski
So, some additional technologies to keep in mind. Um, you certainly could, um, set rules to block transactions. Fns is now doing a pilot to allow blocking of transactions in certain states that are defined that that the state defines as, let's say high risk geographies. So if in your analysis you find, oh, there's a lot of our cards that are being used in counterfeit manner, it's say in California or Florida, you could set a rule to block all transactions for bridge cards in those states, and that let individuals who are traveling there turn off that block. So if I happen to be going to California to visit a family member, I want to be able to shop there with my benefits.

[01:05:39] Chair Jason Woolford (R)
So just to be clear, so if you're on assistance, you need help, but you're going on vacation. Uh, we give people the ability to use these cards in other states.

[01:05:52] Jamie Topolski
Well, currently you can use the card anywhere in the country. Uh, so the the default is to say there's interoperability. Any card can be used in any state. Um, so and sometimes that's, you know, if, you know, I live right on the border with Indiana or, you know, I could be shopping there or vice versa. So there's good reasons to have what's called interoperability, which is mandated by FNS rules. Um, but if you again, if you notice there's a large amount of fraud occurring with your bridge cards in another particular state. This would allow you to say, okay, let's turn off. Let's lock that state. And for the hundred people we have on our bridge cards that need to travel there, we can turn it back on. They can go in the mobile app, they can go on the website, they can go on the IVR turn, you know, turn back on shopping in that state with their card and everyone else benefits is protected. So that's a new something that's not available today that's being pursued. And then likely likewise with terminals that are identified as fraudulent. We could do a better job of proactively looking for those fraudulent terminals where there's a mismatch between the FNS number and other data that we know about that terminal, and proactively cut off those terminals as soon as they're detected, not having to wait for there to be thousands of fraudulent transactions and, and OIG or any other law enforcement agency to spot that and shut it off. But for us, as the processor to proactively shut that off.

[01:07:25] Chair Jason Woolford (R)
It fascinates me to be able to get benefits in the state of Michigan. You have to be a resident in the state of Michigan, but then you can use those benefits in a different state. So some of those monies are not even staying within the state. Uh, so I just wanted to make that as a, as a statement. Also a representative Brook. Oh you will okay. Go ahead. I'm sorry. Go ahead and finish. Yeah.

[01:07:50] Jamie Topolski
The last thing I'll mention is just, um, again, there's newer technologies that there's generative AI that we can start using to detect, um, address, you know, let's just say, um, fraudulent activity that's being done by mailing multiple cards to a criminal's address. The criminal knows that, you know, you may be looking for an exact duplicate address. So what they will do is they will spell the word street completely for one card and then street for another card. They make it very difficult to match. Addresses, so it's hard to know that multiple criminal cards are being sent to the same address. So we can use logic to now start better detecting this type of fraud where we find that there are look, there are some legitimate reasons why multiple bridge cards could go to the same address. It could be a group home, it could be an agency. It could be a shelter for homeless people. There are legitimate reasons why multiple bridge cards go to the same address. But there also are circumstances where criminals have used fraudulent means, identity theft to claim benefits for people that they are not, and then get them all sent to the same address. So there's better tools out there that we're developing to try and help spot that type of fraud. So that's why there is an appendix that talks a bit more about all of the challenges of of EMV and what needs to happen in order to support the chip card standards. It does take a lot of work. It's not simply just adding a chip to the card.

[01:09:26] Chair Jason Woolford (R)
Thank you so much. Representative Bruck.

[01:09:30] Rep. William Bruck (R)
Thank you. Chair. Thank you for being here. You are obviously the expert. I learned something every day and especially about the four digit Pin, the three digit Pin, those variables and how many. That's pretty fascinating stuff. Obviously I do a lot of traveling, have discover, and I get dinged all the time when I travel out of country or even in other states where, you know, they they lock my card or I get that text, I have it set up every transaction I get a text for. So I know when my wife buys. I know when people in my business buy. I keep tracked in that way. But you had mentioned on on slide four it had the six ideas. You talked about the fraud tools that start out with the soft pin restrictions, and then ended with the transition to EMF EMV cards. You had mentioned that the soft pin restrictions are on bridge cards currently in Michigan. I guess my question is these six items that you mentioned or have there on that slide? Are there other states that you are working with that are instituting that? And what is the benefit or what are the positives that you have seen from that? And and just correct me if I'm wrong. In Michigan, they are only doing that first item listed there currently on the bridge cards.

[01:10:46] Jamie Topolski
Unfortunately, I don't know which are being leveraged by Michigan because it's we're not the vendor that the state currently works with for your bridge cards. So there's there's a couple of other vendors in this industry, so I don't know which have been implemented for your current program.

[01:11:03] Rep. William Bruck (R)
Are there other states utilizing all six of these?

[01:11:07] Jamie Topolski
Uh, yes. Although the transition to EMV cards is just underway right now in a few of our states. So the state of Oklahoma is working to implement be our first state to implement chip cards, but several other states have lined up to do that. But every other item on here has been implemented by some of our states. And some of them some of them pick or choose. Um, some, for example, um, may not want the alerts because there's a cost associated with each alert. There's a small, but it does add up when you're talking about that volume of transactions. Others want want all of them. And we do find it's it definitely is an escalating war with the criminals. We've implemented this that second to last one, the adaptive fraud on the IVR. Uh, it really started blocking some of the criminals from calling. Then they implement, then they upgrade their technology so that every call that they do, it changes the number it's from. Somehow they're able to spoof the phone number. That's why we get so many spam calls on every day.

[01:12:10] Rep. William Bruck (R)
Yes, sir.

[01:12:10] Jamie Topolski
Day. And they change the number you block when they change to the next. Um, and that's what they're doing here as well.

[01:12:16] Rep. William Bruck (R)
So it's so on this list of six items, what is the most important item that you would recommend as preventing the most fraud? The quickest amount of time. That would be helpful to us as a state.

[01:12:32] Jamie Topolski
So the quickest is an effective use of the card lock because that's not dependent on any third party, although it is dependent on the benefit recipient to lock their card. The most effective long term would be the transition to EMV cards, because that really does eliminate the opportunity to counterfeit the cards. So from this list, I would say those two would be the strongest ones, the quickest lock and encourage people to lock. Now, what we did on our I don't know, one thing that we have at conduit on our mobile app and on our website, which I'm really proud of, is, look, we all have not we all, Many of us have alarm systems on our home, but we leave our home when we forget to set the alarm. Sometimes I've happened to friends of mine. Um. And the same is true with car locking. You can unlock your car because you're going shopping, but then you forget to lock it when you're done shopping. So now what we added was whenever someone unlocks their car, we put a little prompt up. It says, would you like to schedule your car to automatically lock in 30 minutes, 60 minutes or 90 minutes? And the person selects, I'm going to be shopping for the next hour or so.

[01:13:41] Jamie Topolski
I'll say 60 minutes. Lock my card. They don't have to remember to come back and lock their card. And we found that increase the usage of the card, increase the percentage of time that cards are locked. Because who's going to remember after, you know, they're loading the groceries in their car. They're busy with their kids. No one's got to go back on my mobile app and lock my card again. You unlock it once because even if you go to pay and you're like, oh, my card's locked, you unlock it right there in the checkout lane. You say, lock it again in 30 minutes, you're done. On. So it's not something you have something to remember to do. It's done for you. So that can be a very effective tool. And it's a quick one. But the transition to chip cards. Look we used to get when was the last time you got a replacement card out of the blue. That wasn't because your card was expiring. It worked. It really, really worked.

[01:14:29] Rep. William Bruck (R)
Well, I appreciate I appreciate your testimony. I appreciate all your information. And it it seems like a private industry moves much faster than the government. I can attest to that. So thank you for your influence and hopefully making the government run better. Thank you.

[01:14:44] Jamie Topolski
Thank you.

[01:14:47] Chair Jason Woolford (R)
Thank you. I still have a question for you. Thanks. You're not dismissed, sir. Uh, what would the cost potentially be to Michigan, to its taxpayers, uh, to implement, uh, this, this system? And also, uh, how long would it take?

[01:15:11] Jamie Topolski
That is a question I wish I had an answer for you here. I don't know, um, it is not an, uh. It is not an inexpensive change. The cards are expensive to add the chip. They could be, um, you know, several dollars per card. And it's a big upgrade in terms of the system processing, you know, the amount of data that's on that chip that comes with a transaction greatly increases. So you have to process much more data. So the whole backend system has to now handle additional keys data. That's something we can get to you I just don't know. Off the top of my head it is a multi-million dollar project.

[01:15:49] Chair Jason Woolford (R)
Yes. Multi-million dollar project in hopes to save billions. Yes. I'm not a mathematician, but that seems like a pretty good, uh uh, return on investment. So we look forward to that. Uh, before you go, Representative Carl.

[01:16:02] Rep. Steve Carra (R)
Thank you, Mr. Chair. Similar question is, do you know what the cost would be to, uh, Retailers for the upgrade that have to do to recognize the code for the chips and the EBT cards.

[01:16:15] Jamie Topolski
Yeah, I do not believe it should be very high. Um, there's there should be no need to replace the physical point of sale terminal for the retailer unless they have a kind of a set aside, a second terminal. It's used solely for processing of bridge cards. There's a there may be some retailers that used to be common. I don't think it's very common anymore. But any retailer that has a single terminal today that processes their visa, Mastercard and bridge card transactions. It will be a software update. It's a matter of their supplier or vendor being ready to push that update to that point of sale terminal. And it's going to be it's going to be the state pushing from sort of up high. The retailer is pushing, asking from down below, and hopefully everyone in the middle will get their act together and get those updates written and pushed out. Okay.

[01:17:06] Rep. Steve Carra (R)
Thank you. And then one last quick question, if I may, Mr. Chair, my last question would be from the magnetic strip versus the chip reading. Would there be a higher or lower or equal level of data compiled on an individual in terms of their purchasing habits, where they go shopping, where they buy their food, where they're using their card?

[01:17:30] Jamie Topolski
No additional data? Um, there's no it's an industry. We call it skew level stock keeping unit, skew level data that comes with any of these transactions that I'm aware of. Um, it's it's strictly the exact same data about this is the amount this is the retailer, the date and time. Um, we just have much greater certainty that the card is genuine and the transaction has not been doctored in any way. That's really what we know.

[01:17:58] Rep. Steve Carra (R)
Thank you.

[01:17:58] Chris Carter
Yeah. And, Jamie, I can confirm that on the back end, when we're looking at transactional or data for fraud, we see transactions in aggregate, we don't see individual purchase itemized purchase. We can see person A went to store B and spent X amount of dollars is what we can see. So the amount of data available in the universe Max is exactly the same from a back end perspective. It's all over. It's all around the keys and the encoding of the of the number, the card number itself.

[01:18:24] Rep. Steve Carra (R)
Thank you.

[01:18:26] Chair Jason Woolford (R)
Well, sir. Thank you. Uh, I know that this committee and myself and the taxed citizens, uh, sometimes we lose, uh, the significance of that when we say taxpayers, the people who are taxed on the money they earn. And I are definitely concerned about this fraud that we've seen in these assistant programs, uh, administered by DHHS and which end up on bridge cards. Uh, so I appreciate you being here and your willingness, uh, to help us out in this fight and, uh, to find this, this fraud. So thank you for being here today.

[01:19:02] Jamie Topolski
My pleasure. Thank you. Happy to help any way we can.

[01:19:05] Chair Jason Woolford (R)
And at this time, I'd like to bring up Representative Ron Robinson for testimony. Representative, thank you for being here today. I know you were. You have other committees and other things, but, uh, when you had shared with me, uh, your story, uh, I thought that it would be very important for you for people to hear that, uh, because I, too, have heard stories of people standing in line as we've been talking about these things, where they saw a person with, uh, three different bridge cards, uh, shopping and getting food. Uh, um, those that are in the law enforcement, uh, business saying when they raid a house that they find, uh, multiple cards, not cards that were cloned cards, uh, given or, uh, sold. And there's a price that comes with that. And sometimes, uh, Can be the ultimate price. So thank you for being here and look forward to hearing from you today.

[01:20:07] Rep. Ron Robinson (R)
Thank you, Chair, and thank you to the Committee for hearing my testimony today. I'll keep this short. Um, I wasn't privy to the previous testimony, but when I heard that you guys are addressing and trying to strengthen the structure of this, uh, the system, uh, I had to come and tell my story because we hear stories about fraud all the time. How these people prey on people who are. Were trying to help with this, with these bridge cards. But, um, in November of 2021, a friend of mine was murdered over his bridge card. Um, he lived with with, uh, with a gentleman. And there was some tumultuous relationship going on. But essentially, if if these structures that you're talking about were in place, I think my friend would be alive today. He was killed over his bridge card. And so, I mean, there's not a lot of luckily, the person was sentenced and he's going to be in jail for a long time. But if if these structures were in place, I think my friend would be alive today. So I just wanted to share that with you.

[01:21:03] Chair Jason Woolford (R)
Thank you for that. Representative. Thank you for that. Uh, and, you know, in my closing, I was going to state that this, uh, right now, our our state is truly bleeding so much money in these programs. Uh, and, uh, we have to detect this not only for monetary purposes, but also put in, uh, systems that will help protect people like your friend who rated these benefits. Uh, but because someone knew that they could just use that card regardless. It literally cost him his life. That's true. Those are the people that we're concerned about. Uh, and I know that you know this, but for those that are listening on this committee, I know that, uh, leadership, uh, from the state House to the white House, uh, I know that we are committed, uh, to stopping waste, fraud and abuse and protecting those, much like your friend that are in desperate need of help. So thank you for being.

[01:22:05] Rep. Ron Robinson (R)
Thank you.

[01:22:05] Chair Jason Woolford (R)
Very much. Thank you to each of you on the committee today. There would be no further business. This meeting is adjourned.

END OF TRANSCRIPT