*Indicates written testimony submitted prior to the public hearing per our COVID-19 response protocol

B. HANSEN: Well, good morning and welcome to the Business of Labor Committee briefing by the Department of Labor about unemployment insurance claim fraud, especially in purview and in light to the last year or two when it came to COVID and some of the history, some of the steps or actions, steps that have been taken currently, and maybe some look into the future about how the department is kind of addressing some of these concerns and cases of fraud and abuse in our system. My name is Senator Ben Hansen. I represent the 16th Legislative District in Washington, Burt, and Cuming Counties, and I serve as Chair of the Business and Labor Committee. I would like to invite the members and extra members today to introduce themselves, starting on my right with Senator Day.

DAY: I'm Senator Jen Day and I represent Legislative District 49, which is northwestern Sarpy County.

BLOOD: Senator Carol Blood, representing District 3, which is western Bellevue and southeastern Papillion, Nebraska.

GRAGERT: Senator Tim Gragert, District 40 in northeast Nebraska.

B. HANSEN: All right, thank you. And also assisting the committee is our legal counsel, Benson Wallace, and our committee clerk, Ellie Stangl. So with that, I will invite Mr. Albin to open up and discuss some of the things that we mentioned earlier and kind of leave the floor to him. And then afterwards, when we're done, we'll kind of open up for questions and then kind of go from there, so thank you.

JOHN ALBIN: Fair enough. Good morning, Chairman Hansen, Senators of the Business Labor Committee. For the record, my name is John Albin, J-o-h-n A-l-b-i-n, and I'm the Commissioner of Labor. As I stated in our response to Senators Blood and Day-- oh, I'm sorry. And Senator Day to-- here today too. I'm not used to having extra members. There are several-- and I copied that response to all of you, I believe. There are several answers I will not be able to provide in today's public forum in order to protect the security of our unemployment system. I spoke with Senator Blood on Friday and I remain willing to speak with any members of the committee privately to discuss more specific details. As you're all aware, unemployment insurance benefit fraud is a national issue. While Nebraska has not been immune, we have fared significantly better than most states. For example, in

*Indicates written testimony submitted prior to the public hearing per our COVID-19 response protocol

California, over $810 million was paid to accounts filed under inmate names and Social Security information. In total, California has reportedly paid out $32 billion in fraudulent claims. In June of 2020, it was reported the state of Washington paid out an estimated $650 million in fraudulent unemployment benefits. Impressively, Washington was able to recover $333 million of the fraudulent payments. More current estimates put the fraudulent amount significantly higher. Illinois has identified over 1 million fraudulent unemployment claims. In less than one week, Michigan received over 100,000 fraudulent unemployment claims. The secretary of labor for California, Julie Su, was recently advanced out of committee to be the deputy secretary for the U.S. Department of Labor. And the commissioner of Washington's Employment Security Department, Suzi LeVine, is currently the principal deputy assistant secretary of the USDOL employment and training administration. This information is not shared to criticize those states, but to demonstrate this is a truly national issue that even affects well-run programs. The only national comparison of fraudulent rates are the benefit accuracy measurements [INAUDIBLE] BAM. The national fraudulent rate for fiscal year ending June 30, 2020, which included a good deal of the pandemic, as determined by USDOL, was 400-- 4.35 percent. Nebraska's corrected BAM fraud rate for the same period was 2.43 percent. Nebraska's fraud rate is significantly lower than the national average. While Nebraska certainly has received fraudulent unemployment claims, we've been fortunate that we have not been an early target when new schemes are tried. This has given us the opportunity to learn from states such as Washington and Michigan and react when we have been hit hard. For instance, because of Washington's experience, we were able to quickly deploy a fraud-stop process that required identity verification for individual claims that fit fraudulent characteristics identified in the Washington attack. Additional information from Alabama helped us alert individuals early on of possible fraudulent Facebook accounts designed to mimic NDOL. It's important to understand why unemployment fraud has become a national problem. The federal legislation passed in response to the COVID-19 pandemic created a system designed for fraud. The Pandemic Unemployment Assistance, PUA, program, as originally passed, placed benefit eligibility solely on an individual's self-certification. A bad actor could self-certify that they were in self-employment and currently unemployed due to COVID, and they will receive a minimum of $173 in PUA benefits and $600 in federal pandemic unemployment compensation for this week certified. Additionally, the

legislation allowed claimants to backdate PUA claims to February 2, 2020. This meant claimants could certify several weeks at once and could receive one large payment for all weeks. It's important to note that all states were prohibited by law from verifying this information. Additionally, states faced national and local pressure to implement the new programs and pay as quickly as possible. This was all coupled with a record-shattering claim volume. In 2020, NDOL received 240,105 initial claims, almost six times as many claims as were filed in 2019, and paid $1.2 billion in state and federal benefits to 135,499 claimants. Because there was no verification element and the pressure was on to get payment out quickly, the national system was ripe for fraud. It was not until the Continued Assistance Act passed on December 27, 2020, that states had the legal authority to verify employment information for PUA claims. On January 8, 2021, UIPL 16-20, Change 4, was issued by USDOL. This was the first guidance states received on verifying information for PUA claims. Further, the changes were limited to claims for weeks beginning on or after December 10, 2020. While USDOL is constantly stating the importance of integrity in the UI system, they're also continuously changing the rules. On February 25, 2021, USDOL issued UIPL 16-20, Change 5, and we're told that sometime in the next week we're about to receive a 75-page Change 6. This UIPL created three new reasons for PUA eligibility that are being applied retroactively. Change 5 was issued within just-- with just a few weeks left in the program, as PUA was set to end on March 13, 2020. Under Change 5 guidance, states are now required to give all individuals denied PUA a second chance under the new criterion for eligibility. This means any payment we may have prevented through something other than pure identity verification, such as reporting requirements and work search, will now have a second chance to receive payment. The ever-changing rules around eligibility have made all state systems more vulnerable to fraud. Nebraska, and all states for that matter, have had to continually-- has had-- Nebraska, and all states for that matter, has had to continually evolve its fraud response. The type of fraud and the brazenness of the attacks have-- had never previously been experienced at this level of unemploy-- in unemployment systems. It's even common for them to use state senators and the Ombudsman's Office to attempt to push through their claims. Prior to the pandemic, NDOL had existing fraud prevention measures in place. However, in response to the unprecedented nation-- nationwide attacks, NDOL has continuously reviewed and adjusted our methods for fraud deterrence. Initially, the

most common type of unemployment fraud was unreported earnings and the false-- and false PUA information. This meant the individual bad actor filed a claim as themselves and falsified their own claim information. Nebraska's existing processes, such as cross-matches with the State Directory of New Hires, the National Directory of New Hires, wage cross-matches and prisoner cross-matches served to detect and prevent this fraud. Then the pandemic introduced widespread identity theft as never before seen. Under these identity theft schemes, bad actors from all over the world used previously acquired, stolen identity information from prior data breaches such as Equifax, Target, Home Depot, etcetera, and used that information to file a fraudulent claim using the victim's information. NDOL implemented several measures that generally reduced the amount of payments made under these attacks. First, NDOL requires participation in reemployment services and eligibility assitant-- assistance programs for selected unemployment insurance claimants not attached to the workforce. Nebraska was one of the few states that continued this requirement throughout the entire pandemic. Solely by requiring claimants to report to the job centers as part of our reemployment efforts, 5,523-- 23 potentially fraudulent claims were stopped. This prevented over $54 million of potentially fraudulent weeks from being filed. Additionally, Nebraska was one of the first five states to reinstate work search requirements and has one of the most stringent requirements in the nation. Nebraska requires claimants to certify five reemployment activities per week. We have been a longstanding member of the National Association of State Workforce Agencies and an early member of its UI Integrity Center and Integrity Data Hub. Nebraska is one of the seven original pilot states for NASWA's Suspicious Actor Repository an IDH. As a pilot state, we participate in the development and requirements for the system starting in late 2015 and signed our first MOU in February of 2017. Nebraska was the first state and is still one of the only three states to implement and use the automated connection for submitting SAR bad actors. Since this time frame, NDOL has been submitting and receiving data to and from SAR. Recently, NDOL has been working with our vendor and the Integrity Center to utilize even more functionality. We've actually lost four employees to re-- as recruits to NASWA, three of whom now work directly with NASWA's Integrity Center. Through weekly calls with the states coordinated by NASWA, Nebraska learned valuable tips in reducing the pandemic-- in reducing fraudulent payments and was able to adapt throughout the pandemic. Since August 2020, NDOL has required all new PUA claimants to provide

proof of identity by a government-issued photo ID or the equivalent. This activity alone prevented $16 million in pending fraudulent claims from being paid; and had the bad actors succeeded, payments would have exceeded $85 million. As the state saw more and more success in detecting and preventing identity theft, bad actors switched their approach to hijacking valid claims. Bad actors have gained information about individuals with valid claims to determine the answers to the password security questions and reset their passwords. Once the password is reset, they take over the valid claim. This information is typically received through phishing schemes, previous data breaches, and social media sites. Since alerted to this type of scheme, Nebraska has implemented multifactor authentication. Once implemented, every single claimant had to pass multifactor authentication to access their claim. If an individual fails multifailure-- multifactor authentication, identity verification is required to gain acc-- regain access to the claim. This is just a sampling of some of the things Nebraska had in place and has done in response due to fraud throughout the pandemic as we learned more about the fraud attempts. It's important to note that to date there's been no known breach of Nebraska's unemployment system. The federal response to UI fraud has also evolved over time. Changes in legislation have helped; however, the system-- unemployment systems are stuck between the balance of getting money to individuals quickly and delaying payments to prevent fraud. You all have had calls and emails from citizens wondering where their payments are. Every state has had to try and find the right balance. For example, we saw an increase in calls and correspondence from your offices when we implemented multifactor authentication on April 9, 2020, yet for week ending 4-10-21, we compensated 14,994 weeks. This includes 6,983 regular UI claims, 2,532 PUA claims, and 5,479 PEUC claims. For week ending 4-17, we compensated 13,878 weeks. This includes 60-- 1-- 6,128 regular UI claims, 22,571 PUA claims, and 5,179 PEUC claims for a two-week total of 28,872 weeks' pay. So despite the increase in calls, payments are still going out and real claimants are successfully accessing the system. On April 3, 2021, iss-- USDOL issued UIPL 16-21, Ident-- Identity Verification for Unemployment Insurance Claims. Based on this UIPL, Nebraska was ahead of the game. Most of the items recommended in the guidance were already in place in Nebraska. Since 2020, NDOL has required all new PUA claimants upon filing to report to NDOL with proof of their identity and later expanded this requirement to all PUA claimants. If a claimant does not provide the information, they're denied benefits

for a failure to report, as UIPL 16-21 outlines. This has stopped over $16 million in fraudulent claims of actual weeks claimed, prevented an additional $85 million in fraudulent weeks' claims from being paid. Now a government-issued photo ID is the equiv-- or the equivalent is required for all new UI claimants as well. As encouraged in UIPL 16-21, Nebraska has utilized for several years the NASWA Integrity Center and Integrity Data Hub. Prior to the pandemic, if fraudulent activity was suspected, NDOL required claimants to report and provide sufficient identity verification. In May of 2020, we significantly increased the tools we use to identify suspected fraud when we implemented increased data analytics to stop fraudulent overpayments. The information we cross-matched against align-- aligns with UIPL 16-21, was issued almost a year after we made those changes. Proof of our success detecting and preventing fraud has continued to be demonstrated as we take additional steps to further detect and prevent fraud. NDOL has provided the Office of Inspector General with the data from our entire system to compare against a database of all states' data. The OIG dedicated a task force to analyze all states' data including banking information, emails, phone numbers and Social Security information. From the OIG review of Nebraska's 240,105 claims filed, NDOL was only given 2,079 possible fraudulent claims. Less than 1 percent of the total claims filed in Nebraska came back as possible fraud. With that information, some of the-- within that information, some of the claims may have already been established as fraud or may not be fraud at all. For instance, a claim in multiple states created a hit. Of those hits, several were only filed in one other state, so a claim may have correctly filed in both Iowa and Nebraska. Additionally, they examined email addresses of claimants and used very broad terms. For example, "John.Albin@gmail.com," which is not my email address, would create a hit because it uses a period between my first and last name. Furthermore, NDOL issued 1099-Gs and to date it's only received 52 valid individual complaints of identity theft through our 1099-G fraud-reporting process. NDOL is not naive. We have experienced fraud at an unprecedented level during the pandemic. However, we are constantly working to better deter fraudulent activities. NDOL's team has proven to be very adaptable to the ever-changing times. Fraud is not a matter we have taken lightly. The unprecedented attacks on Nebraska's UI system are extremely concerning and we are working with the Nebraska Attorney General's Office, the State Patrol, and also federal authorities in regard to those claims. With that said, NDOL's efforts have been very successful when compared

to the national data. Our team continues to be dedicated to fight this fraud battle, all while ensuring much-needed unemployment insurance benefits are made to Nebraskans. That concludes my testimony and I'd be happy to answer questions and will-- that will not put our internal security risk-- our claimants at risk. Thank you.

B. HANSEN: All right. Thank you. And so with that, I will open it up for questions from the committee. And then we'll kind of just kind of play it by ear and kind of go from there as we go along here, if that's OK with you, Commissioner.

JOHN ALBIN: My morning is yours.

B. HANSEN: OK. All right. So with that, I'll open up for questions from the committee. Yes, Senator Blood.

BLOOD: Thank you, Chairperson Hansen. And-- and thank you for coming out today. I know this is an uncomfortable situation. I do want to say that I've enjoyed working with your staff and especially Katie Thurber, who has been exceptional, so I do want to make sure that-- that that's said out loud. Now with--

JOHN ALBIN: Thank you.

BLOOD: --that, I also have so many more questions since I heard your testimony. And-- and I feel confident that these are pretty commonly known issues, that we're not going to be hurting your security in any way.

JOHN ALBIN: OK.

BLOOD: So in your letter, you stated that prior to the pandemic, you utilized CAPTCHA and then upgraded to a more-- and anybody using your site knows that you use CAPTCHA and then upgraded to a more robust system, which is reCAPTCHA. And my concern is that it seems like a lot of things weren't implemented until the pandemic. Would that be accurate as far as having a really big concern with our security when it came to people's identities and unemployment fraud?

JOHN ALBIN: I don't think that's entirely accurate. We've certainly made a series of upgrades to the process as we've gone through.

BLOOD: Right.

JOHN ALBIN: You know, the current system came on board, online in October of 2019. I think it's substantially more secure than the system that preceded it. We have upgraded as we've gone through, as we've detected fraud. It was never a large number and we never had the concerted attacks. And quite honestly, the original FPUC, the $600, combined with the PUA, gave people more incentives to try and defraud our system than ever before. And so I think every state has adapted quite a bit in the last year. And, yes, the pandemic caused us to make a lot more changes. Well, you can see from the timeline that we handed out to the committee we've made a lot of changes in a fairly short period of time to adjust. Yeah, the wage cross-matches, the prisoner cross-matches, the SSA cross-matches were all pretty adequate in the past. They were not adequate in the face of the level of fraud that we faced in the pandemic, so we have upped our game to fight back and try and limit the fraud.

BLOOD: So a lot of what you're talking about would be more concerned with the local fraud, like inmates, as it showed up in your audit. But we know that we're working with international crime rings; specifically, Nigeria seems to be one of the most efficient crime rings. So when I look at the timeline, I look at the beginning and I have a lot of questions. I'm trying to keep this in perspective. So I apologize. I know it's a lot of information. But wouldn't you say that CAPTCHA is basically useless against nefarious automated attacks? Wasn't that-- wasn't that kind of opening the door at the very beginning because we just had CAPTCHA and really nothing that really addresses the suspicious activity that came from overseas?

JOHN ALBIN: Well, at least, as to bot attacks, if you ask the folks at NASWA, there are several states that have had much lower rates of success for the bot attacks than others. Three of the states that stand out are Nebraska, Louisiana, and Tennessee, and they all utilize the Geographic Solutions, COTS solution for that, so-- and I'll be honest with you, they've got security prevention measures up there at their level that I don't even know about, because obviously John Albin didn't call them up and say, we've got to do something about bots. They already had stuff in place to do that, so--

BLOOD: But-- but weren't there free online sites that allowed ne'er-do-wells to-- for instance, there's online CAPTCHA-solving services, like I found GRIS, Alchemy, Clar-- Clarifai, NeuralTalk. So it was really easy for-- I mean, a grade schooler could go in and

pretty much surpass our original security when we had CAPTCHA. And then with reCAPTCHA, so that's a solving service. right? And it's really easily integrated, which is why so many people use it. But the problem with reCAPTCHA is that it allows Google to-- to basically give us surveillance, like Google knows everything that's happening now, so now we have another portal of information going elsewhere. Is that something we're comfortable with?

JOHN ALBIN: I guess I am very comfortable with reCAPTCHA as a deterrent. It is certainly not something that is going to stop all fraud, but it certainly makes it more difficult for the automateds. As to the individuals, it's probably-- you could still keep attacking away, but it does prevent most of the automated fraud.

BLOOD: But-- but isn't part of the algorithm for reCAPTCHA the fact that if I have a Gmail account, then I'm a lower risk score?

JOHN ALBIN: That may be for CAPTCHA but not for reCAPTCHA.

BLOOD: Hmm. See, my research shows differently, that that was one of the areas of weakness when people thought they were improving security is that it just opened a different door of security issues. So--

JOHN ALBIN: Well, reCAPTCHA requires you to match pictures, so I'm not sure how having a-- the Gmail and Google could research the pictures that it randomly throws up.

BLOOD: Well, but reCAPTCHA allows the Google to-- allows Google to analyze how users are navigating through the website. That's why it's an additional security as opposed to just CAPTCHA, which is just about the pictures--

JOHN ALBIN: Um-hum.

BLOOD: --which also could be, if I'm a person with a disability or a person without a disability because I'm a ne'er-do-well, I can get the software that basically solves the puzzle for me. Right? I mean, it's on CAPTCHA. That's an easy thing to do. I could do that. I could leave this office right now and do it. So-- so here's the question that I have. So we know that reCAPTCHA is a risk score system, right? So are we embedding that V3 code on all the Web pages or just on the pages of the forms and log-in?

*Indicates written testimony submitted prior to the public hearing per our COVID-19 response protocol

JOHN ALBIN: OK, you're going-- asking an IT question beyond my knowledge. I'll have to have someone get back to you on that one--

BLOOD: OK.

JOHN ALBIN: --as to where it's embedded.

BLOOD: Because in order for it to be--

JOHN ALBIN: I know that every morning when I go onto it, it pops up, then I need to match the pictures.

BLOOD: OK, so-- so that's one of my concerns that I'd like an answer on, is that we are-- are-- are saying that reCAPTCHA is robust, but I think it brings secondary security issues. So, for instance, if you look at the reCAPTCHA's cookies, they kind of follow the same basic logic as like-- like a Facebook "like" button. If I have a site and I put a Facebook "like" button on my site, what a lot of people don't know is that anything that happens then on that site where I've put that Facebook "like" button now is information that is fed to Facebook, so they know what's going on on my website. So that's-- they use that same kind of cookies for the reCAPTCHA and that creates concern. So when we embed things like that, it's really an online grab, kind of like-- like Accelerated Mobile Pages, which is kind of what happened to media, is that AMP took away all the great people who used to go and actually get real news on the media. So I'm really concerned about that being one of the issues that we use when we say-- when we talk about security. I know that a perfect storm was created, that you guys had an increase in claims, that there was pressure to speed up the claims, that mobile banking apps complicated the issue. I know in some cases there was prepaid debit cards for some recipients and I know that that, though, also paved a much easier access for these gangs from other countries and-- and local criminals, but I'm more worried about the people outside of our state. And we know that on Telegram, that there's a step-by-step scammer's guide that showed Nebraska was targeted over and over again and that we were paying out. And that's a cloud-based anonymous message system that anybody in this room can access. So I still see little leaky things that I'm worried about, and I'm not sure-- and I know I have a lot of questions, I'm sorry, but your letter caused more questions for me. So I want to know about the V3. I have concerns about that we think that reCAPTCHA is-- is that beneficial, and then I have concerns about the timelines. So I

know that in November, that's kind of when the Secret Service put up the red flags, because I read all those articles; some of them I think you referred to in your packet here. I saw that we were audited in-- or we received a report in December that also showed that fraudulent claims have been paid out, a substantial amount of fraudulent claims. And then in January, we were lucky enough to receive a grant, $1.2 or $1.3 million from the DOL to help us with fraudulent claims. Does that sound right?

JOHN ALBIN: That could be right on the time line for the-- when we received, but I don't think our efforts started in November. As I remember, we were doing stuff. You know, I mentioned that the lowball-- or the low-tech. Providing-- requiring people to show up and provide proof of identity started in August and reCAPTCHA is not the only tool that's used.

BLOOD: Right.

JOHN ALBIN: There's also a 16-factor, at least 16-factor, nightly batch process that's run against all claims and additional--

BLOOD: [INAUDIBLE]

JOHN ALBIN: --measures have been added after that, so it becomes-- you know, reCAPTCHA, is it-- would I say that that would be the only fraud-detection item you need? No. And that's why we have others behind it analyzing the claims. Our vendor also does-- since it does UI in three different states and PUA alone in about 20 other states, which is the program that's been hit the most hard by the fraud efforts, they're doing all their nightly analytics, as well, for all of those 20 states involved, which is one of the advantages of being within our consortium of states, of sorts. It's not an official consortium. We just use a common vendor. But that PUA program is running in all 23 states right now. And so they're using-- they use analytics and information that they're fed by all of those 23 states to constantly upgrade their security efforts on that end.

BLOOD: Did they also encourage you to do two-factor authen-- authentication prior to just two weeks ago? Was that something that they had recommended prior to the fraud, after the fraud had started happening? Because it seems like two-factor would have been kind of

the standard several years ago, but we didn't do it until two years ago.

JOHN ALBIN: Well, I don't think dual factor has been a standard-- industry standard in the unemployment world since day one because our systems were all designed to make it fairly claimant friendly. I think that the recommendation, consultation, do you want to use this, that occurred-- it probably was-- I want to say February or March. It took a while to get it stood up. And most of that was on us rather than the vendor, but it took a while for us to get it stood up.

BLOOD: But they had just recommended it or had they recommended it quite a while ago?

JOHN ALBIN: The first time I recall us discussing it specifically was in February or March, somewhere in that time frame.

BLOOD: Of 2021?

JOHN ALBIN: Yes,

BLOOD: I know that there might be other people that have questions, so I'm going to stand down for a little bit here.

B. HANSEN: Yep. Yeah. And so open it up to see if anybody else on the committee has any questions at all. I have one question as-- also want to ask real quick. You kind of mentioned a little bit in one of your paragraphs about the OIG report that we had on the amount of files, claims-- claims filed and the amount that were possible fraudulent claims--

JOHN ALBIN: Yes.

B. HANSEN: --was less than 1 percent. Now, comparatively, how-- how-- how do we compare to other states when it comes to like the amount of possible total fraud claims com-- compared to the amount of claims? Do you know, by chance? It's not huge. If you don't know, I can always get back [INAUDIBLE]

JOHN ALBIN: The OIG doesn't mean-- as far as I know, didn't share everybody and all states composite. It just-- it shared with individual states. Every state provided its entire UI file for fiscal year '20 and I think in-- with the federal fiscal year, I believe we

went through September with the last of the claims have filed. Every state provided that file to the OIG. The only official fraud statistic that I'm aware of was the BAM one, and according to BAM we're about half the national rate.

B. HANSEN: OK, because it's-- it-- to me, it sounds good we had less than 1 percent of possible fraud, but then I don't know, unless-- you know, I'm trying to-- unless I have some kind of spectrum about where other states were at, so I'm just kind of maybe-- I just asked that question, just kind of curious about that.

JOHN ALBIN: I will look and see if we can find some other information on that. I would guess that 1 percent is on the lower end of the spectrum.

B. HANSEN: OK. All right, thanks. Any other questions?

GRAGERT: I would have a question.

B. HANSEN: Yes, Senator Gragert.

GRAGERT: I'd be interested in before COVID. What kind of-- what kind of fraudulent cases were there before or did you even track it?

JOHN ALBIN: We tracked it. Actually, before COVID, the fraud rate was about one-half of 1 percent. It's always been there. It was not large. You will see in every recession that the fraud rate goes up because the fraudsters figure out that, because you're handling a high volume of claims, you're probably not going to be able to spend as much time with them as you normally would. I think during the Great Recession the fraud rate went up to 1.5 percent was the peak year of the Great Recession, 2010, I believe, then it dropped down after the Great Recession ended. We were back down at a half-percent the last time that I look-- for the last year that I'm aware of prior to the pandemic.

GRAGERT: With the pandemic, you know, came a-- a-- a rush, a tremendous amount of unemployment cases or, you know, applying using Facebook and all these others, it had a convenience for everybody to get in and get their money fast, which also helps out the fraudulent part of this and-- and with convenience comes along increased fraud?

*Indicates written testimony submitted prior to the public hearing per our COVID-19 response protocol

JOHN ALBIN: Well, convenience lends itself to fraud that-- and that's always the tension that you-- that you fight. I mean, all of your offices probably received a call from probably several claimants over the last spring about they're so slow processing my claim, why can't they make it faster? You know, we've had people that, with the dual authentication, it's caused its own little glitch in the process because some people go in there and, I don't know, where they're not taking it seriously. Ticked off when they start the process, they'll create a weird email account that they forget that they even created and then-- and they'll change cell phones. They don't bother to update their information, then when they get a dual authentication, they can't dual authenticate because the stuff that they have in the information-- or they didn't update their file, so we don't have current information and then that results in a call to our office or your office. The amount of unemployment fraud shared through social media was certainly bigger this time just because you create all these fairly anonymous sites where people can exchange all sorts of information. Another factor that was really different this time than we saw on any prior time, and it's been difficult for every state to deal with, has been the large security breaches at places like Equifax and Target, because all of those have information right down to the gritty details on every claimant. I mean, I personally experienced it in our family. My son lives in Massachusetts. His boss comes up to-- or his HR department there at MIT comes up to him one day and says, John, why did you file this claim? And he said, I didn't. And that person had every bit of information about him that was needed to file the claim. On the regular UI claims we had-- we have the traditional backstop of we send out the separation information request to the employer. And then if they say, but Sally is still working here, we immediately start investigating the claim. We're a little bit inhibited in that effort and in this particular recession because a lot of the HR offices were closed. And so those SIs, as we call them, separation information requests, sat on somebody's desk because they weren't there or in the inbox where they weren't working. So we didn't have as good a backstop as we normally have from employers in that regard. The other side of it, and, you know, where everyone believes most fraud exists, is on the PUA side. And that's because that traditional backstop of you send the SI out to the employer and the employer says, but they're still working here, doesn't apply in PUA cases because you're claiming self-employment, so you are the person. So the same person claiming to be unemployed is the same person who's

supposed to verify that you real-- are a real person. So the PUA program has been a particular vulnerability for everyone. I think every state has been really frustrated with USDOL in regard to the PUA claims. You know, early on we all said, you can't do this without some sort of income verification, this is nuts. USDOL said, we don't think the law allows us to, then just to give you a little inside baseball, we do PUA programs administered by agreements with USDOL and-- and you and part of the black letter of the agreement is you have to follow USDOL guidances. And USDOL told us, not once but twice, that you could not verify information for these people. That was the reason that we went with the requirement on-- starting with the suspicious claims in August of last year, to have people show up because, you know, USDOL told us we couldn't in-- verify informa-- verify income, so we said, OK, they didn't tell us we couldn't verify identity. And they keep putting in all these UIPLs they send at us "Fraud prevention is paramount," and it's like, yeah, but you keep opening the door for all the crooks. And just to show you the continued mixed messages we get and part of our frustration with USDOL, the Biden administration came in and changed the PUA rules and that's their prerogative. Elections have consequences. They can do what they will. Then the U-- and that's fine. They have that prerogative. It's a little confusing because they didn't just say we're changing them prospectively. They said we're changing them retroactively to February 2 of 2020. OK, that's problematic when you consider that we had 65,000 claims and 770,000 weeks of claims certified during that time period, so that's a big caseload. But they're paying for it and so we'll start working for-- and then, you know, we have our usual "preventing fraud is paramount to us," a portion of the letter. And so in these cases, you're talking about 52 to 60 weeks' worth of benefits that you can go back and retroactively redetermine eligibility. Well, PUA, like the unemployment program, is something that you're required to weekly certify your eligibility. You got to tell them whether you-- if you're-- from July 12 on, we required work search. You got to tell us what you're doing to try and drum up business. You got to tell us what income you earned and all of that. So USDOL comes around and then send us a note and says, oh, by the way, if somebody wants to do one certification for all 60 weeks, that's fine by us. So tell me how in the world that doesn't just open itself up to fraud, because every week is an individual week of certification of eligibility. So it's been a frustrating process for us on-- on the federal side in that regard. And then you have competing federal programs besides because

FEMA administered the lost wages assistance program. FEMA said, we don't care if USDOL is opening up the PUA claim and we don't care if those weeks apply to the time when the LWA benefits were available, but because we think the rules have changed, you can't pay LWA benefits for those time periods. So we're going to-- if-- when we get this process worked through, we're going to have to recode something in the system so that two claimants that are eligible for the same week starting July 27 through September 6 of last year, one claimant is eligible for that week for PUA and gets LWA because they had a appeal pending or some such; and another one who recertified under the new rules that the Biden administration put in place will not be eligible. And somehow our computer has to be figuring all that out, so it's going to be a coding nightmare in the process.

GRAGERT: With the increased frauds-- and I suspect with the increased frauds, of course, that's why we see the timelines of all the increased security measures. So I guess-- I guess at some point you got to take and assess the risk and go. There's never going to be a perfect plan, I understand that, but what-- at what point, you know, if you're going to try to get the top security, how long is it going to take to get the payments out to these people? You know, I-- I-- I-- where is the give-and-take, that fine line you got to find?

JOHN ALBIN: Well, with the current measures that we have in place, I think we do fairly well. Under normal circumstances, USDOL wants you to get out 90 percent of your first payments within 21 days of the claim being filed. For the month of March, we beat that federal-- or we didn't get the first payments, but we got the adjudications and we were darn close on the payments. We were up in-- we were in-- want to say in March we were in the 83 to 85 percent rate, so we were pretty close to what USDOL says you should do in normal times, so I think we struck a balance in that measure. I'm guessing that within the next few weeks, we will probably do another evolution in terms of the security because, you know, the fraudsters are really good at their criminal activities and every time it's kind of like a chess game: Every time we make a move, they make another one to try and exploit. So we would be foolish to sit on our laurels and say-- you know, I think we've done a good job, but do I think we can just say, OK, run up the victory flag and say the game is over? No, it's not-- it'll be a battle throughout the end of this-- of these federal programs. And, you know, I guess technically they end on September 6. I'm guessing they won't, but-- so I'm guessing we're going to be fighting this

battle for a long, long time. And then, you know, it's just like every other recession. When the recession is over, you know, we'll spend a couple years looking at what happened and figure out errors we made, things we could have done better, things we'll do different the next time we go through it, so, you know, yeah. Anyone is rightly concerned-- a right to be concerned about the level of fraud and we need to work hard to stay on top of it. I think we've done a good job at this point. But a good job now is probably not going to be a good defense tomorrow or the next day or whatever. So we'll be constantly evolving our efforts. That's part of the reason we were one of the founding members of the UI Integrity Center with NASWA. It was a good deal that we did that. It cost me an employee that was a really valuable employee because one of their main persons in their fraud unit now is one of my former employees. But I guess that's the way it goes, but-- so we've tried to stay-- and the nationals-- we've exchanged a whole lot more information at the national level now than we ever had before. And I think being part of a multistate consortium will lend itself--Pennsylvania and Iowa will soon be using the same vendor that we have now, so, you know, the nice thing about being in these multistate groups is that you learn from their mistakes. And fortunately, Nebraska is small enough that we usually don't get hit first. We were really benefited greatly by Washington State. They have a really large weekly benefit amount, plus a dependents' allowance, and so they hit them early on and hit them hard, $650 million and-- but a lot of that stuff, by the time they tried the same tricks on Nebraska, Washington had already tipped us off, so we were already in a position to deal with it. So that's been an advantage of being a smaller state.

GRAGERT: It's unfortunate fraud has to happen, but it does. And like Senator Hansen, I don't-- I don't really know what 1 percent means at this time, but it sounds like we need to commend you for the-- you and your staff for how vigilant you are on this. Thank you.

JOHN ALBIN: Thank you.

B. HANSEN: Any other questions? Yes, Senator Blood.

BLOOD: So we were talking numbers. Why don't we visit the audits.

JOHN ALBIN: Oh.

*Indicates written testimony submitted prior to the public hearing per our COVID-19 response protocol

BLOOD: I think that's a good place to go naturally next. So what do you have-- you spoke briefly about the audits when you and I met on Friday that you didn't think they were accurate, but the audit showed a loss of tens of millions of dollars of fraud. I don't know if that's included in the 1 percent or-- but to me, that seems like a lot of money.

JOHN ALBIN: Well, a million dollars in a $1.2 billion program, which is what 2020 was for us, is not a huge number. I mean--

BLOOD: We-- well, when we're always fighting for property tax and killing bills with fiscal notes that have like a $100,000 fiscal note, to me, as a senator, tens of millions of dollars of taxpayer dollars seems a lot of money.

JOHN ALBIN: Well, it'd be a lot of money if it was sitting in my bank account, that's for sure.

BLOOD: Yeah, mine as well.

JOHN ALBIN: So, you know--

BLOOD: And I think to the average person on the street, that seems [INAUDIBLE]

JOHN ALBIN: --Senator, in all honesty, no level of fraud is ever acceptable. But at the same time, it's like a retail outlet, a Target or a Wal-Mart, they don't ever like people to shoplift, but they assume in their business process that there's going to be some, just-- and that's how they're going to-- and it's going to be the way in the-- you know, if you create a system to the point where it takes four and five weeks to get out the first payment to every claimant, that really works a disservice to the claimants that are out there because they've just lost their job and they've got rent or a mortgage to make, and so you need to work in speed. And the whole UI system is set up to assume that there's going to be an error rate. I mean, the improper payment rate that the Office of Management and Budget assigns to all programs is 10 percent, so they're saying 10 percent of your programs-- or your payments can be made in error and you're doing just fine. It's probably a little higher than I would like to see, but-- and I think every other state administrator would share. But you kind of accept that given the ground rules where we're supposed to

prioritize speed, that we have to-- there's going to be some fraud involved. As to the state audit, I think their numbers were grossly exaggerated. And it's-- you know, they've-- their figures were-- I don't know what-- I mean, about $7 and $8 paid they were claiming was subject to question, but yet when you look at the 1099s that we've sent out to individuals, we've sent out 135,000 1099s. So far, we're at 52 complaints that have been officially filed that someone stole their ID and filed their-- a claim against them when they weren't entitled. So I'm guessing that the number-- those numbers don't seem to correlate with the figures that the State Auditor had. And of course, the State Auditor works-- like the BAM statistics, they take a fairly small sample of a large program, and this year was larger than most, and they take a look at it and make projections based upon what's in that pro-- or what they find in their small sample.

BLOOD: So-- but the fact that it was a small sample and they were able to show tens of millions of dollars, to me, that seems kind of the opposite of what you're saying.

JOHN ALBIN: No, they take-- they didn't find tens of millions of dollars within their small sample that they took. They took the results from their small sample and extrapolated that over a large-- the entire universe, and then they came up with their large number. There's a difference there.

BLOOD: But didn't they show actual examples of people of-- that received overpayment or people that had-- I mean, like within the audit, they showed actual individuals, Nebraskans that they used as examples. Isn't that true?

JOHN ALBIN: Yes, they did find individuals who were overpaid. Some of the cases were just flat-out mistakes by our crew. We went from basically 25 adjudicators resolving claims before the pandemic to-- I think we peaked out at about 250 to 300, which meant you brought a lot of people on in short order and a lot of claims were processed by inexperienced people and-- and lots more errors were made than normal.

BLOOD: So I wish we had more time so we could actually walk through it line by line. So we know that your employees handle sensitive information every single day. And because of that, I mean, really, the risk factor has always been high just based on the type of-- of information that you guys handle. Wouldn't you say that's accurate?

*Indicates written testimony submitted prior to the public hearing per our COVID-19 response protocol

JOHN ALBIN: The risk factor was a lot lower before PUA. And I don't want to just keep beating a dead horse, but PUA changed the whole game because before, you always had the employer community acting as the basically second house or the review process. They would say, did the person-- first of all, the benefits were based upon wages that employer reported and he couldn't change that wage amount unless that amount was appealed and then got actually cold-entered into the system. PUA basically was self-attestation. Also, in the past, you know, when somebody would file a claim and the employer says that person still works here, so this is bogus, and they would get back to us, we would know that before the first dollar got paid. With the PUA program, there's nothing similar to that back there because there is no backstop of the second entity reviewing that claim, the employer community entering the claim. So it's-- in the past, those were much easier to stop because it was regular claims; it's a system. And again, if an employer has been reporting wages for somebody for ten years, it's pretty lock solid that that person really does work for that employer. And then all you got to get down to is adjudicating the nature of the separation. With the PUA programs, you have no comparable backstop in the system and USDOL has done its level best, up at least until December 10, to prevent you from doing some reasonable applications. I mean, just the PUA program, basic eligibility hasn't changed since the program was created in March, and we're now waiting for our sixth set of instructions on just how to do the PUA program, things-- and USDOL, it's things like this pen-- do penalties apply to people who file a fraudulent claim? For ten months, USDOL told us, no, we can't apply penalties to them, suddenly said, oh, we went and reread the law, you do apply penalties to those people. So we have to administer the program in accordance with their guidance and it's been less than clear.

BLOOD: So that leads me to-- and I'm going by memory so you can correct me if I have the number wrong. In the letter that you-- response you sent back to Senator Day and myself, you had kind of walked through what you knew as far as what monies were still owed and what you had collected in 2020. It wasn't all of 2020 yet, but from what you had so far. And didn't it say that it was either $24 or $26 million that was still not collected as far as fraudulent claims?

JOHN ALBIN: Overpayments, yes; fraudulent claim, not all of-- that includes all overpayments, whether they're fraudulent or nonfraudulent. So, you know, if a-- if an employee certified they were

eligible for that week but didn't do the work search they're required and we discover that upon audit, that's an overpayment, but that's not typically a fraudulent overpayment. So the $26 million in overpayments is-- the amount that we still have pending is not all fraudulent overpayments; it's just overpayments.

BLOOD: I-- I mean, the concern-- one of the concerns I have is that when you compare us to like Wal-Mart, I mean, Wal-Mart's not dealing with taxpayer dollars. I mean, we're responsible for our-- our taxpayer dollars, and that's one of my concerns when we talk about it in that fashion. But you had referred to, in the information you sent to us, working with the State Patrol and the Attorney General's Office to put together a protocol on how to handle this. Was that not put into place before the pandemic?

JOHN ALBIN: We have referred cases out to county attorneys in local fraud cases since I started with the department 30 years ago. So that is nothing new, referring out fraudulent claims. Occasionally we end up working with federal authorities in regard to some of the claims because there are federal issues involved. The difference this time is most of the fraud before is what I would call individual fraud in the sense that didn't-- went back to work, didn't bother to report to us, and then went ahead and claimed benefits for 10, 12 weeks on the systems. So those were individuals and were pretty easy to determine and to track down, and we could pretty much lay out the information the local prosecuting people are needing. In this particular case, it's going to be a whole lot different because a lot of it is the Internet fraud. And so we're going to rely upon the State Patrol and the people in the Attorney General's Office to help us do a little more sleuthing, because we could do-- we can say these claims look fraudulent, this is what we've got, but we really don't have the bandwidth within our department to do the level of cyber criminal investigations that the Attorney General's Office or the State Patrol could do. And then after we get-- and we've referred over some cases, I think they're over there now trying to work through to see what we can and can't do and what will and will not work. We have a lot more that we can, once we've got it established exactly what works for them in terms of a prosecution, then we'll be able to start making more referrals to us. They've been very cooperative with us in the process, very helpful. I think we started first working with the Attorney General's Office back in, I want to say, April of last year. That was the first contacts we've had with them so-- and they've been very

responsive and very helpful in the process. It's just a big issue that it's going to take time for us to work through.

BLOOD: But no real protocol then put into place yet, just more conversations and some back-and-forth and--

JOHN ALBIN: Well, we've put together a sample file and sent it over to them for-- to work through, so I don't-- they told us what to put in the first set of files and we'll see where that goes from there. We put it all-- we've provided all the information that we were asked.

BLOOD: Yeah, it's unfortunate they're not here to walk us through how they're going to be handing this-- handling this. I mean, if I was on your security team. I mean, the things that come to mind for me are, you know-- and it looks like some of this is being addressed, which is fantastic, by the way. But, you know, we need to make sure that anomalies are flagged, so out-of-state banks, obviously, duplicate email addresses, which you did address, multiple names being used on the same bank accounts, which you're starting to address, foreign IP addresses.

JOHN ALBIN: We've never allowed a claim to be filed with a foreign IP address.

BLOOD: Excellent. And then repeated computer serial numbers and techniques that help to mask those numbers, that was one of the issues that I'm still not finding real clear in here.

JOHN ALBIN: I think we're actually doing that.

BLOOD: OK.

JOHN ALBIN: And the multiple bank accounts, that's not just recent; that's been ongoing for quite a while.

BLOOD: And I look at some of the things that you say you've been doing, and as you stated in your response letter to both Senator Day and I, my office has handled more U-- UI complaints than all of the senators combined and it's exhausting. And so the fraud was probably brought to light-- to us, it was more magnified, obviously, because we had so many people that were desperate that we helped find groceries for, that we helped get their utility bills paid for, some of them transportation. We became almost a DHHS minioffice to help people get

help and it shouldn't have happened. That shouldn't have happened. Part of it was because other senators' offices weren't helping, which is unfortunate. And I'm not going to point fingers at anybody, but a lot of the frustration that these people were going through, I-- I really feel strongly, could have been avoided. And we have key people in your office that my staff has worked with who have been exceptional. But even with the magnitude of claims that you got, you hired how many extra staff and, what, three organizations to help you with that?

JOHN ALBIN: I think it was up to around 300 additional contracted staff, plus expanding our own substantially. I think we added probably 100 to 150 internally and then about 300 out-- externally. We worked with Nelnet, Robert Half, and North End Teleservices out of Omaha.

BLOOD: But hadn't Nelnet had its own data breach within just the last few years?

JOHN ALBIN: I'm not aware of one with Nelnet. I just-- there's been a lot of data breaches in the last few years. It could have happened and I wouldn't-- and I don't know about it.

BLOOD: No-- no doubt. Yeah, I would be concerned hiring them, if we're worried about fraud, if they've had their own data breach, or are they only utilizing our system or do we use a portal? How do they work with that?

JOHN ALBIN: No, they utilize our system only. So if somebody hacked the Nelnet system today, they still wouldn't be into our system.

BLOOD: Unless they were using certain surveillance software on their computers which allowed them to follow whatever you're doing on your system, which is always a concern, but, you know, that's a concern on our own computers. We have Mac Airs and for some bizarre reason, IT decided to put Chrome on our computers, so now Google knows everything that we're doing, as well, as opposed to sticking with Firefox. So there's a lot of things with IT in the state that I don't understand that I think opens us up to continued fraud, not just in your department but in other departments that deal with people's personal information and tax dollars. So unfortunately you're just the one that's in front of us today, so I apologize.

*Indicates written testimony submitted prior to the public hearing per our COVID-19 response protocol

JOHN ALBIN: Lucky me.

BLOOD: So I don't want to keep asking questions if there's other people that want questions answered.

B. HANSEN: That's fine. I-- I might actually have one more question here I'll ask and then-- because we're going to be-- we'll be stopping the briefing probably in about the next five to ten minutes, so that gives us time to kind of get ready for session and to add any closing remarks that you might have. But maybe just for clarity for the taxpayer and just for us in general, when it came to the pandemic unemployment assistance that the federal government created, that is not Nebraska taxpayer dollars. Right? That's just all federal government money?

JOHN ALBIN: That is all federal government.

BLOOD: It's the taxpayers'.

JOHN ALBIN: Just a brief recap of the funding of all the programs, all the state admin dollars are federal; all of the-- for regular benefits, for PUA, for PEUC, and for FPUC, that's-- the only benefits that are paid directly by Nebraska employers would be the regular state benefits, which, you know, you're an employer, you file a quarterly return. We take-- we assess a tax on those wages, then those are deposited to the federal Treasury in the U.S.-- in the, excuse me, Unemployment Trust Fund. So other-- you know, there are no General Fund programs in the program. There are a lot of federal dollars. And then to the extent-- you know, for accounting purposes, the money that's paid out of the federal trust fund counts as federal funds, which is why the payment of regular funds shows up in a CAFR audit because it's considered a federal fund, but that those contributions, as they're so wonderfully described, those are the ones that come directly from Nebraska employers. The rest of it is-- comes out of the federal grants and, of course, every Nebraska-- and the PUA program, I have no idea how the feds plan on paying for that, because unlike the unemployment system, where there's a basic tax set up at the federal level, where every employer files their quarterly FUTAs and pays their four-- quarterly tax. There's nothing comparable on the PUA side. They've just been paying it. I have no idea what account they've put it in. All I know is that it shows up in our funds, that we can draw it down. It's all federal funds.

*Indicates written testimony submitted prior to the public hearing per our COVID-19 response protocol

B. HANSEN: And I appreciate that, I guess, that relation, because I always have a great concern whenever we cannot verify information. And when the federal government then tells us we can't by law verify information, I want to make sure it's not Nebraska taxpayer money that we are not being responsible for if the federal-- federal government tells us we can and cannot do something, so--

JOHN ALBIN: That is correct. We're still free to verify and we do verify on all claims.

B. HANSEN: OK, just want to make sure, so-- and then one more thing. Is that commonplace for the federal government to say, look, we're going to give you money to help out with unemployment or some other kind of program, but, however, you cannot verify information? Is that-- is that new or have-- have they done that in the past before? I'm just-- maybe just for a little [INAUDIBLE]

JOHN ALBIN: It is totally unprecedented. It has never occurred in the past. If you look back at the Great Recession, the feds' additional payments in that case were $25 a week and it was only on regular state unemployment claims. There was nothing comparable to the PUA program. I understand the reasons that they created the PUA program. But unlike the unemployment system, which has an 80-year history and we've learned a lot about how to administer it, there is nothing comparable in the PUA system and-- to the PUA system and the prohibition on verification of income that they had into that program and the limitations they have on it now.

B. HANSEN: OK, and I appreciate that and I think Senator Blood was kind of alluding to that, as well as making sure that we're responsible for taxpayer money and we can verify where it goes, making sure we can decrease the amount of fraud that we're having. And so I would hope on the federal level that they would kind of have that same kind of philosophy when it comes to taxpayer money, because it still is our money. And that's why it concerned me, like something that's never happened before, and the-- and our inability to actually garner information to make sure the money is going to the right place is a little concerning to me. So I at least apprec-- appreciate your clarifying on that. So with that, I'll-- Senator Blood, do you have more questions?

BLOOD: Yep.

B. HANSEN: OK.

BLOOD: And, yeah, I just, again, want to clarify, all tax dollars, be they federal or state, belong-- come from the taxpayers, so let's make sure we're really clear on that. So do you require all of your software vendors to offer the multifactor capabilities?

JOHN ALBIN: We really just have the-- primarily the one software vendor other than the State of Nebraska OCIO.

BLOOD: And that's a "yes" then?

JOHN ALBIN: Yes.

BLOOD: OK. So do you feel now that this has happened, that when it comes to like device forensics, data analysis, and-- and the proprietary controls that we really have to put in for suspicious activity, do you feel that we're where we need to be? And-- and hindsight-- and this is a hard question and I apologize in advance, all right? Hindsight, even though we only had limited fraud before, wouldn't this have been something that maybe we should put into place before the pandemic and had lost all that money?

JOHN ALBIN: Well, hindsight always has the virtue of being 20/20, so, yeah. Are there things that I wish we had had in place earlier? Yes. You know, we were doing a good job before in handling the type of fraud that we were facing. The new types of fraud I don't think any state was ready for, and we have done, I think, a good job of getting in position to now address those issues. I think we've-- every state has learned a lot that we will utilize going forward. Once this pandemic process or pay-- or unemployment program ends, there will be a lot of things that we'll do going forward. You know, just in the process of the claims, you know, we've always cross-checked driver's licenses. It's a good way to validate the individual's identity. What we didn't anticipate and no state anticipated with the Equifax and the Target type of breaches, and I don't-- I just used those two. There's been a slew of companies that have been breached. I don't want to sound like those two are the source of all our problems. That sort of information that before was very easy to verify is now always very available on the dark web and not very expensively, I guess. Someone told me $2. I don't know. I--

*Indicates written testimony submitted prior to the public hearing per our COVID-19 response protocol

BLOOD: I did.

JOHN ALBIN: OK, I have not gone out on the dark web and I'm not going there, so I don't know what the going prices for an SSN and that sort of information on the dark web. So I don't know. So if they-- they're-- we have-- in the process of the system now, we require people to either come to one of our local offices that they don't have a lot of computer equipment of their own or to upload a valid driver's license. We will probably make more innovations in that page-- in that process as we go forward in the future, because some of our sister states have seen some-- a lot of characters from The Office showing up on their drive-- as the photo on the driver's license. So it will be an evolving process as we go forward. We're doing better, a whole lot better. We were good to start. We're doing better, but we need to do more and we'll have to do more as we go forward, because the cyber criminal world is a whole different world. The amount of data that gets captured, I mean, standards that we used in the-- without-- the financial industry, I mean, your mother's maiden name used to be kind of a gold standard for verifying information. But with social media and being able to go out and figure out who your relatives are, coming up with a mother's maiden name really isn't all that hard anymore. You know, the fraudsters, they threw up a ton of Facebook-- false Facebook pages. The Facebook folks have been really good working with our national association and USDOL to take some of those down and prevent them. But they created a lot of false sites, you know. You know, when it went up there, "Contact Senator Carol-- Carol Blood and she'll help you," that was legitimate because she does and she-- and you have helped a lot of people. But a lot of those sites were nonprofit for unemployment claimants, and basically what they wanted to do was enter the information so they could capture it and hack your account. So it's-- criminals have no conscience, apparently, and they have exercised no restraint in trying to steal people's identities in this process.

BLOOD: So I'm going to-- only because we're running late, I'm going to kind of close this with one question and a comment. And you've touched down on it a little bit, that that was from our Friday meeting, is that what people have to understand is that these Nigerian-- and I-- and there's more than Nigeria, but that seems to be the biggest culprit that I'm finding on the dark web-- is that these Nigerian crime rings pay $2 in cryptocurrency, so we know that that's being used as well, to buy somebody's name and Social Security number,

thanks to things like the Equifax breach. And there's a huge directory of information; probably people sitting in this room right now, our names and Social Security numbers have been purchased. And then they know that a lot of the things that they're going to utilize are things like CAPTCHA that they can get around with software. So the people put in two-factor and then maybe the second question is, what's your mother's maiden name? They're going to be able to go to Ancestry.com or one of those ancestry sites and find out your mom's maiden name. And then they might also find out what high school you went to, so they're going to know what school mascot that you have, because we know that almost everybody's annuals or yearbooks, whatever they call them, depending on your generation, are online. So I was actually talking to a professor of computer science yesterday and-- and we were kind of walking through the different ways that we can prevent fraud. And he was really frank and is like, you know, no matter what you do, as long as they have that Social Security number, until we figure out that one particular issue, we're always going to be fighting this. So the concern that I have for the Department of Labor, the concern that I have for DHHS, the concern that I have for the Department of Revenue is it seems like we so often wait until there is a huge crisis to really step up security. We know that all of this informa-- I mean, I'm just a 60-year-old grandma and I found all this out, right? I saw the hit lists that were put out that showed Nebraska clearly was paying out $300 effectively on a regular basis and, yeah, because we only pay out $300-- $300 in general, that we weren't as big a hit as like California or Washington State, but we were still hit and we were still promoted as an easy state to hit. So the -- the question I have for you is going forward, and I know you've touched down on this a little bit more, are we going to address the what-ifs better? Because we know that criminals have nothing but time on their hands to figure out every day how to screw us over and most of us don't live in a world where IT is always on our brains. What-- what can we do better? And I'm not saying that you've done it not any better than a year ago, but I question whether we're where we need to be to make sure that this just doesn't happen. And I know we can't completely, like I just said, completely stop it. But what can we do better? And one of the things I'm really worried about is I think the protocol should be put into place between the AG's Office and the State Patrol because never say never. We don't know that this is not going to happen again, right?

*Indicates written testimony submitted prior to the public hearing per our COVID-19 response protocol

JOHN ALBIN: Oh, it'll happen again. I mean, fraud's been with the system since the first day the system went up. It's more prevalent. And the international actors that we've seen recently, with ability to move money between continents quickly, are all new. And that was one of the reasons that we became a-- one of the earliest members and then a-- one of the trial states for the Suspicious Actor Registry [SIC]. We have every intent of, and so do the other states that we're working with through the UI Integrity Center and the-- and-- and the IDH to keep working on these claims. In fact, USDOL is now contracting with NÁSWA using IDH for its security measures. And so we have every intent of using them as we go forward to evolve because it's going to be an iterative process. The system is good today, not as good as it needs to be, and will be better tomorrow, and that's just the way you've got to approach it.

BLOOD: Thank you.

JOHN ALBIN: Thank you.

B. HANSEN: And I would maybe like to share just more on-- more on a personal level that I do appreciate you. And I can speak for myself and maybe even the rest of the committee. We do appreciate you and your department's hard work, actually, and vigilance in respect to the unprecedented amount of claims that you've seen the last two years. It's a lot to work through with the new hires that you guys had to do. So I do appreciate all the hard work everyone has been doing, and especially in the environment of ever-evolving fraud. [INAUDIBLE] like I say, it's a chess game sometimes, and so providing some history and context today for us and for the Nebraska taxpayer moving forward, so I appreciate that. With that, that will close our--

JOHN ALBIN: All right.

B. HANSEN: --briefing for today so we can get back, go to session. And so again, I appreciate you coming and that will close our briefing for today. Thank you.

JOHN ALBIN: All right. Thank you, Senator.