Identity Theft and Scam Prevention

Webinar Transcript

Right. Well, let's do this. Good afternoon. My name is Becky MacDicken and I am with National Disability Institute. You are joining us today for Identity Theft and Scam Prevention: What's Changed, What Hasn't? This is brought to you today by our Financial Resilience Center and Experian. Next slide. Yes. So thank you to Experian for their generous support for this webinar today. And, again, our Financial Resilience Center we'll talk about in just another minute. Next slide. But first we're going to take care of some housekeeping. As you can probably see, we have ASL interpretation. It's been arranged for this webinar. There will be two interpreters for the event and they will switch off periodically. If you need to view the ASL interpreter, navigate to the menu bar at the bottom of your screen and click on "interpretation". Select "American Sign Language" to view the interpreters in a separate video pane. Next. So audio and captions can be accessed using computer audio or by calling in by phone for today. If you select computer audio, please make sure your speakers are turned on or your headphones are plugged in. To call in for audio, please dial 877 853 5257. And the meeting code for today is 881 7954 5189. Real time human captioning is being provided. The captions can be found by clicking on the CC button in the Zoom controls at the bottom of your screen. If you don't see the captions after clicking the CC button, please alert us via the Q&A box. Next. For any questions and technical assistance, please do use the Q&A box. We can answer most things there. They'll be addressed by the presenters, myself and Mike, if time allows. And we have people behind the scenes answering as well. If your question isn't answered during this webinar and you have a burning issue, please use the Q&A box. But then if that doesn't work, you can email Liz Layman at elayman, L A Y M A N, at ndi inc.org. And please do note, this is being recorded.

The materials will be available on our FRC, Financial Resilience Center, page within one to two weeks. We will also be sending out the slides. Next slide. So, you're here with National Disability Institute. If you are not familiar with us, we are a non profit dedicated to building better financial futures for people with disabilities and their families. We are the first organization committed exclusively to championing economic empowerment, financial education, asset development, and financial stability for all people with disabilities for the past 20 years. Yes, we are celebrating our anniversary. So some of the things that we do. We build capacity of the field through training and technical assistance. We train service providers to be better at disability inclusivity. We drive systems change by implementing models that can then be replicated throughout the country, such as resource mapping. We are testing innovative approaches to financial empowerment, different counseling methods. We are leading research to uncover barriers and opportunities for people with disabilities. And we are advancing change through public education and policy development. Next slide. So our Financial Resilience Center, we are the one sort of semi hosting this webinar today. Please go to financialresiliencecenter.org and look through all the resources on our website for people with disabilities. It was built during COVID and meant to be a place for resources to help everyone emerge stronger financially, whatever the situation might be. Next slide. And a quick overview of FRC. We provide a lot of up to date information, alerts, and different financial tools and resources. We do analysis of federal policy and the impact of those policies. We have a lot of resources provided in a Q&A format under topic areas of interest, although we are undergoing a website revamp in the moment. And then lastly, we do have a place where you can sign up for our emails to make sure you are alerted to webinars such as this one and other ones coming up in the future, receive a newsletter, blogs, all those kinds of things. So please do feel free to sign up. I believe they just put the email sign up list in the chat for you or the Q&A, so you are able to

do that. Plus, we will be sending these out with live links after the webinar today. Next. So, our presenters today are myself, Becky MacDicken with NDI, and Mike Bruemmer, who is the Head of Global Data Breach Resolution, that's a mouthful, with Experian. So we are excited to be here today. And before I turn things over to Mike, one more slide about today's agenda. I do want to point out that two years ago we held a webinar with Experian, and Mike was there as well, called Avoiding Identity Theft: Financial Resources for People with Disabilities. That recording is still available on our website, and most of the information in it is still incredibly useful and timely. So if you need a primer on identity theft, you can always go to that, but we are still going to hit the highlights today. We're going to talk about those things that haven't changed, what's new, give you some resources, and then answer your questions. So, with that, I believe I'm going to turn things over now to Mike Bruemmer.

>> Thank you very much, Becky. We'll go on to the next slide. I'm going to start with the discussion of identity theft and scams and the difference, but we will be talking about specific recommendations, how to protect yourself, what scams and identity theft threats have taken place, and everything in between. And as Becky said in the introduction, please give us any questions in the chat. If something is urgent you need it answered, that's fine, too. We can be interrupted. And I look forward to tag teaming with Becky on this.

>> Oh, I think we might have a poll question, too.

>> Okay, well.

>> Sorry about that. Go ahead, Shelby. So, if you would be so kind, do you know the difference between identity theft and scams? Yes or no? Not sure? Please fill that one out. And then we're going to share the results. Looks like everybody's in. So we're going to say

70% said yes, 8% said no, and 15% said I am not sure. So, all right, I will stop sharing, and now we can move to the next slide.

>> So for the 23% of you that either said no or that I'm not sure, here's the correct answer and the simple way to think about it. And I'm going to start, actually, on the right hand side, because a scam is just one way that identity theft can occur, and it's not necessarily that it happens because you may have a scam that defrauds you out of money or takes some other information but actually doesn't result in identity theft. There's also data breaches, nation state attacks, ransomware attacks that aren't necessarily in the category of scams. But think of the obvious thing. You get a link that you're not familiar with about something you're interested in, and then they go ahead and ask you to click on it, and it downloads something bad on your computer. Identity theft is when personal identity information, or PII, actually gets taken and then used to impersonate you to be able to either gain money, gain reputation, gain an insight to, let's say, intellectual property, create a fake ID, open a mortgage, anything like that. So they're not mutually exclusive, but they are tied together. But scams always don't result in identity theft, and identity theft can come in many directions. But scams just is one of the threats that everybody is facing today, especially during shopping season. Next slide.

>> And I actually think we might have one more poll here. Our research team has been on overdrive. [Chuckles]. Okay. So now, have you or anyone you know been a victim of identity theft? Yes or no, or I'm not sure. And then the last one, have you or anyone you know been the victim of a scam? Yes, no, or I'm not sure. And lastly, have you or someone you know been a victim of Social Security or Medicaid, Medicare benefits fraud? Yes or no. So I'll give you a moment to answer all three of those questions. You can see where we're heading with this. And most people have seen or know somebody who's been a victim of identity theft or a scam. Not so much in the Medicaid well, still pretty high in Medicaid. And we're

still getting a couple more answers. All right. We're going to end the poll then. It looks like activity is ending. But, yeah, we've got a high concentration of people who are very familiar or know somebody who has been a victim. All right, thank you. Next slide.

>> Okay. So we're going to start with what hasn't changed. And, of course, scams right now around the holiday season are by far the most important thing in anybody's life. And these scams are 'too good to be true' deals during the shopping season. I mentioned malicious links earlier, and they could be malicious links that are sent to you by text, email, or other means. Also, it could be malicious websites out there that have scams on them. Fake marketplace sites, social media sites are also very popular. And then during shopping season, the good old delivery notification scam. So if they don't get you on the front end, they send a fake delivery notification that says, hey, we need some more information to be able to deliver your Amazon package or even deliver your DoorDash. And you click on it or you answer it, and you provide information, and there you go. One of the things that I was telling Becky right before the webcast was we just released our 2026 data breach industry forecast. And there were six predictions, and five of those six involved AI, artificial intelligence. And that's what's been the biggest change in this whole identity theft and data breach space over the last 12 months. It's the newest frontier. It's transformative. And recent Experian data says that 82% of consumers see AI driven scams as their number one threat. These are super realistic websites using deepfake audio and video. And this has just gotten to a point where you, as a human, can't tell the difference between audio and video that is manufactured using AI versus the real person, and that's a problem. There's also AI driven bots that will mimic human shopping interaction and pose as humans to be able to defraud shopping websites. Most recently, we had Cyber Monday this week, and I believe it was a tipping point for AI because you had high traffic, you had a sense of urgency, and you had more social engineering attacks powered by deepfake audio and videos than we've

ever seen before. And last but not least on this slide, what hasn't changed is that disabled consumers are in the top three target areas for identity theft. Very much in the same group, young adults, why children are susceptible, because it is a virgin or new identity or new credit file that can be used and abused. Senior citizens, because they're not as technologically savvy and don't understand some of the things that may be presented to them. And then, for obvious reasons, disabled people just because of awareness of a physical or other disability that may prevent them from understanding and accessing or not being able to access the right tools. Next slide. Becky, this is yours, I think.

>> It sure is. So some of the latest data that we're getting on general identity theft trends. The Federal Trade Commission, or the FTC, received about 5.7 million fraud reports this year, and that includes 1.4 million identity theft cases. The most common type of identity theft was actually government documents or benefits fraud, with almost 400,000 cases, and that obviously disproportionately affects individuals with disability who rely on public benefits. Next slide. A couple things to protect the disability community from fraud. Obviously, we know identity theft occurs, and it can be because of an over reliance on caregivers or third parties to manage finances for a person with a disability, leaving them vulnerable. That personal identifying information, otherwise known as PII, is stolen and used. It can be used to apply for credit. It can be used to file taxes or procure medical services. I will tell you on a personal note, I have a young adult who is on the autism spectrum, so I have many friends in this circle of people with disabilities. And several of my friends have had caregivers in their home for their children, and those caregivers have stolen personal information and, you know, created fraudulent accounts. So I know of at least two of my close circle that that's happened to. There are a lot of financial scams out there, and we're going to get into this a little bit more as well, but they trick people who may not have the cognitive ability to understand what's going on into giving out money.

There are a lot of other scams such as romance scams, is actually a huge one for the disability community. You've got someone who wants connection; they want to interact. They're lonely, and it goes for all of us. But if you're looking for romance, these websites, the dating sites are rife with people trying to scam you. So be very careful. And we're going to get more to investment scams and employment scams in just a minute. So actually, I'm going to turn it back to Mike, I believe. [Chuckles].

>> Yes. And please, on the next slide, these two slides go together, and Becky touched on this, and this is specifically focused in on the disabled community and what's happening, and the top of the list because of special benefits is the government impersonation. A lot of disabled people are dealing with the government to get benefits, especially medical benefits, and the bad guys know that. And so they will impersonate the agency that you're working with, whether it's federal, state, or local, saying, hey, your benefits are being held up, or there's a change in your benefits, or whatever, to get you to click on a link or to answer a phone call as well. New scams purporting to give lots of money for working from home. We know in the disabled community a lot of people have been homebound and have had to work from home, and so they're targeting that as well. Along with that, job postings and interviews. Fake websites for that. Someone impersonating someone from out of the country to be a person in the United States interviewing for a job and vice versa. Then 'too good to be true' medical health care services and discounts as well as specific to Medicare and Medicaid fraud. That's all really relatively new. Some of it's been around for a while, but this is current from my last query with ChatGPT and my identity theft experience. Next slide, please. So here's some specific examples. VA disability benefits. And these were from Puerto Rico, but there was an insider working in the VA stealing lifetime benefits. A third party administrator was a benefit administrator had their founder and CFO take $100 million out of their fund. Of course, insiders as well with nursing care or home help staff

scamming people where they're incapacitated, either by impersonation and/or deception. There was a recent ring of caregivers in a state hospital that was in Florida that stole PII from the patients because they started it and they worked both sides of patients in room, patients leaving, even taking benefits from people that recently passed before they could be put on the death master file with the Social Security Administration. And then worst of all cases is family members impersonating a loved one who is in trouble and needs help and money. Unfortunately, identity theft still has almost 50% of the cases of identity theft initiate from someone that knows that person, whether it's family or close friends. Next slide. Back to you, Becky.

>> Yeah. So we've been getting a lot of questions about cryptocurrency. I'm not going to tell you what to do specifically, but personally I don't want to touch the stuff; I'll tell you that. But some key warnings and recent developments we want you to all be aware of. So some of the common scams. Again, impersonation scams where there's, you know, somebody impersonating a government official, a bank or even a celebrity. Has everyone seen the Tom Cruise deep fake? That's creepy. But they trick you into sending crypto for whether it's, you know, for an upfront business opportunity or something else. It could even be charity and it's a trick, so don't fall for it. Sending crypto is a red flag in and of itself in my opinion, but we want to be careful there. There are a lot of crypto investment scams going on where there's these promises of getting a high return for your money and what they do is it's called pig butchering. They actually the fraudster is working with someone and they're yielding fake returns and so then the person puts more money, and the victim puts more money in; they're fattening up the pig. And then when there's a lot more money in the account, that other the fraudster strikes and takes all the money. So they're called pig butchering schemes. Be very careful. You really should make sure you're verifying who somebody is. If they say they're an investment person, you can do that through there's

websites where you can check that, BrokerCheck, things like that. Then the romance scams, I already mentioned it very briefly, but there are so many people who are again looking for connection. You get online and suddenly this very charming, very, you know, photogenic person starts texting you, and you think they're out of my league. Sure enough, one, the grammar starts to go downhill, although with AI that's getting better, so be careful. But we know of people I know of someone here in Pennsylvania, who's an older woman, lonely, got tricked into giving somebody over $100,000. She'd never even met him in person. The worst part was someone came back around a few months later after the person had disappeared, the scammer, and said, that was my brother; he's missing. Can you help me look for him, and got another $40,000 out of her. So we need to be paying attention to grandparents or people who may not be as aware or savvy of the technology. And then lastly, the blackmail and extortion. I actually received a very creepy email one day addressed to my father, and it said, we know where you live and we know what you've been looking at on your computer. Now click here and send us money or we're going to release this. And I know that my father, being 87 years old, wasn't doing anything he shouldn't have been. The fact that he had a picture of his house was very creepy. But we've got to pause when we get any kind of these kinds of opportunities and think about who this is, who's emailing, verify what's going on and just don't panic. And when you kind of take a breath, I think you'll realize many of these things are scams. Next slide. Whenever Bitcoin ATMs get involved, again, my little Spidey senses go off. So it's being used increasingly in scams. If someone asks you to pay for something via a Bitcoin ATM, be very careful. Victims are usually told to deposit the cash into the machine, and what happens is the machine then sends that cash in Bitcoin form, which is a digital form, out into the ether, and basically it disappears. Yes, it leaves a digital footprint called blockchain, but it's very, very hard to trace. So I know that the FBI is trying to break some of this stuff up, but they

reported losses of $250 million last year in Bitcoin scams. So a couple other tips on crypto and Bitcoin. Don't send crypto to settle debts, pay taxes, or resolve legal issues. Real authorities are not going to ask you to pay via crypto or even gift cards. Be very skeptical of unsolicited investment offers or emotional appeals, and double check those sources. The Federal Trade Commission has a great guide about cryptocurrency and scams, and the link will be live when we send these slides out to you. Next slide, please. So a couple things on the AI. I think, again, Mike already touched on some of this, but the voice cloning for grandparent scams is getting really good. Scammers use AI to mimic a grandchild's voice saying, "Grandma, I'm in trouble. I'm in prison, or I'm in the hospital." And for whatever reason, people don't check with their actual children or the grandchildren directly and have fallen for this to the amount of $21 million over 40 states in the last year or two. These deepfake impressions, I mentioned earlier, they create realistic videos; people send money. So be very careful what you're watching. The phishing emails we used to warn about have gotten better. Because of AI, the grammar tends to be a little bit cleaner, and things are more personalized, but if you get an email asking for money or click on this link and provide information, just stop, pause. Be aware that synthetic identity fraud is happening now, and that is where AI is generating fake identities, which then can get you fake jobs, fake loans, applications for loans, things like that. And lastly, again, fake job offers on shopping sites - or and shopping sites. We know that there are some jobs that aren't out there. Anytime someone asks you to pay up front to work from home, that's usually a red flag, and we want to be very careful on those shopping sites. I don't know if anyone has ever typed in Amazom.com instead of Amazon, but sometimes there is a spoof site out there. I know Amazon has tried to keep that away, but I've actually seen it before, the right timing. So be very aware when you are going to websites that you think you trust. Make sure you've got the right website address. Sorry, next. [Chuckles].

>> All right.

>> Go ahead.

>> I think I'm going to take this one, and I'd like to continue on that thread about synthetic identities because I mentioned earlier about our 2026 predictions, and one of them is actually called "more real than real", and these are super synthetic IDs. If you remember Blade Runner from 2011, it used a tagline, "more human than human". And, in fact, AI allows the hackers to create super realistic fake birth certificates, driver's license, using deep fake audio and video. Not only have they increased 300% year on year in 2025, but 91% of these super synthetic IDs will avoid conventional detection. So it's a real issue. Anytime we talked about clicking on links, you need to also worry about don't answering any calls from callers that you don't have either in your contact list or caller IDs, if you recognize. I still recommend all my calls outside my contact list go to voicemail, so I don't pick those up. Second, use two factor authentication. That means in addition to a password, you have a biometric, like a thumbprint, a retinal scan, a text even to your phone and to get a code. Be skeptical of anybody that's soliciting you something you're not expecting. And if they're asking in a secretive manner or immediate action, it's even higher alert. I would also say pass the word on, especially to your moms and dads and younger kids. I know my kids don't understand voice cloning because it only takes about 10 seconds for someone to take a voice print of Becky and then they can go ahead and impersonate Becky with any language model that you need. And last but not least, it's important to give back and giving back means file an internet complaint with the IC3. It allows you if you think you have been scammed or going through a scam, you should go through a police report. But if you file with the Internet Crime Complaint Center, they get the word out to say, here's the latest scam that's going on or latest use of AI, and it gives other people that may not be aware the chance to be forewarned. Next slide. All right, which threats are current? And again, from a

lot of the slides that Becky and I have put up there, we've already talked about some of these. Again, this new supercharged, synthetic ID is really important. Tech scams and now with tax season approaching and end of year, you have don't forget you have 'benefits to use' scams or unpaid tolls. I think 61% of the people in the US got some sort of request for unpaid tolls in the last year because it was going around and repeated. The deepfake phone calls we talked about, and then last but not least, good old email and snail mail. There's still letters that you get whether it's what Becky talked about. I got a picture of my kids from them playing sports that says, "We understand that you're a pedophile. Would your kids want to know that?" And they sent it to my house. Of course, it was handwritten. My name was misspelled. It was actually not a good scam, but it still happens. And those threats are current. I would also add to this list, because of end of year charitable giving, there's a lot of charities that are out there asking for donations right now. And about one third of all charity requests are actually fake charities and they're scams. So be aware of those.

>> I've even heard of people getting fake Santa outfits in red buckets. So be very careful there. [Chuckles]. If you want to make sure your money is getting to the right place, maybe send a check to the known address through the website or something of that nature. But again, check the website. Some of the red flags besides a Santa suit. We like this acronym. Remember SURF. So again, part of it is just pausing. But there's always a scare tactic with these scams. You know, we're going to report you to the police. The IRS is going to audit you. You miss jury duty and there's a bench warrant out for your arrest. They're trying to scare you. And then there is this urgency, the you. That is just we're trying to get you to act now without thinking quickly. So by remembering to pause, again, you can sort of say, wait a minute. Does this seem real? Is this legit? And you can sort of take that beat and find out what's happening. The R, it's just random. It's never any you know, what have I done? I think almost every scam we've talked about today, I feel like there's been an attempt to

reach me for some of those. So it's completely random. Just be aware. That's the best thing you can do and just watch out for the phishing, whether it's the text, which that's a little bit newer than the emails. Make sure if somebody's asking for personal information, don't give it if you don't have to. And even, I know that people even talk about when you go to the doctor's office, sometimes they ask you to verify your social security number. The last four digits of your social should suffice. But we want to be careful where we're saying that out loud in public. We want to be very aware of all the times people are asking for that information. Next.

>> And prevention must. Being the guy who works for a credit bureau, I'm going to always start with freeze your credit file at the bureaus. You have to do it individually at Experian, TransUnion, and Equifax. It's free. It doesn't take very long. There's also apps with each one of the bureaus that you can have on your phone as well to lock and unlock your file. But you can do that over the phone with any agent. It's easy to do. I also recommend using a password manager. And the one I use is Keeper, but there are other ones. 1Password is another one. But password managers are great because they will give you automatically on a website and generate a long and complex password you don't have to remember. And then the password manager will store that in 512 bit encryption so that nobody can hack into it. I'm a big fan of shredding any documents older than 60 days. You don't need them for any other reason. Get rid of them. Put on the spam blocker on your cell phone. Most of the providers can block phone calls and screen phone calls or have them go to voicemail, and I think that's always a good plan. I'm not a fan of keeping the landline if you don't have to because all that we're going to do now I still have a landline for my alarm system, but I have the caller ID come up on my TV and you'd be surprised how many spam phone calls I get to my old landline. Always verify and never trust. And what that means is verify identities that you're dealing with, verify shopping websites and providers, and never trust,

never assume and take for granted that you need to not trust people that might be even from a stolen email be sending you a legitimate email. So I call it being Chicken Little. Vet any offers that you have with another non family member to make sure, hey. Is this really the bank that's asking me to do this? Or is this really the Social Security Administration to do that? Don't react to something, but go get a second opinion just to make sure. If you think it's suspicious, it very well might be. I mentioned also earlier two factor authentication and then filing a fraud report with the FTC. If you see scam attempts, again, this gets communicated around, put out in public relations material so you know who's being scammed by what most recently. Next slide. Unfortunately, people do become victims of identity theft and in the latest Experian study, we found that, in the last year, 16% of the US population reported that they have been a victim of identity theft. I go back to even if you haven't frozen your credit before you become a victim, for sure freeze it at each one of the bureaus afterwards. Check your free credit reports annually and Experian can provide you those. I also recommend our IdentityWorks protection membership because that will monitor your credit file 24 by 7 without you having to do it and it will alert you. If you have accounts that were impacted, meaning you think, hey, I was shopping with my Chase card at Kohl's or whatever, close those accounts. Change the passwords on those accounts. You need to file a police report, and the reason filing a police report is important, it is your official record of becoming a victim. It will help you with recouping any money or information or whatever with an institution particularly financial institutions will require a police report. Also, if you have an IdentityWorks membership that has identity theft protection insurance and to you get that insurance, you're going to have to provide a copy of the police report. Then also, I mentioned earlier, again, file a report with a federal trained commissioner, FTC.

>> Mike, it dawned on me that one of the things when I was working with my colleague, Shelby, down at Family Caf , and one of your colleagues, one of the questions we got a lot was, especially in the disability community, a lot of people are credit invisible because they've never had credit. I just wanted to know if you had any thoughts about whether it's good to not be credit invisible and get something established? Or to prevent identity theft, is it better to stay credit invisible? I hope I'm making sense of my question. [Laughs].

>> It makes total sense and I would give the same advice to a parent that has children under the age of 18. If a credit file is not already created, meaning you're credit invisible, there is no advantage to creating a credit file in terms of protection for identity theft. It's better to be as invisible and not as much not have that. You don't want to go ahead and create a credit file to freeze the credit file because it's better to have no file than a frozen credit file, just in any case. Not that a freeze isn't going to work, but why create something when you don't need to? That's a really good question and pretty easy to answer.

>> Okay. I think we might have another poll now. We do. So what methods do scammers use to steal your identity? So there's anything powered or supercharged with AI. There's text scams. There's deep fake phone calls, email, physical letters sent through the post office. All of the above. So that's the first question.

>> Can I answer, Becky? I guess I probably should. [Laughs].

>> Yeah, go ahead. Then the second question is, will using two factor authentication on your accounts help protect against identity theft? Yes or no. I'm not sure. And a third question here, what do you do if you or a family member received a suspicious call from someone asking urgently for money? Be skeptical; don't share your personal information; report suspicious activity to local law enforcement or the FBI; all of the above. All right.

>> I think people were listening to what we said.

>> I think they were. I'm very impressed with our answers. All right, I'm going to end that poll. And we can go to the next slide. We just have some other tools and resources. These will be sent out, again, with the slides and everything. So you'll get those when we send this out. Is there another poll now? I think there might be one more question. And then we actually have a question in the chat. Let's see. Oh, would you like to be added to our listserv so we can follow up with you about this and other projects? Yes or no?

>> Yes. Yes.

>> Oh, that's a good one. A question says, a person SSI back paid check for their child, the check was stolen and cashed. How should they proceed? So I don't know if we've got let's see. That's a stolen check. I would contact the Social Security Administration first and foremost so they're aware that that's happened and that Lori might have gotten an answer. Do we have any opportunities? I'm looking at the Q&A, sorry. Well, this will be on replay, so I'm not sure if you're looking for further training on this. Lori's got you covered in the answers. She's going to take care of you. So any other questions right now? I think we're up to the question slide.

>> Yeah. And one of the things we were talking about in our pre meet before the webinar, I think the question was asked about, is a mobile device more risky than, let's say, even an iPad or a laptop or a desktop? And the answer is yes because so many people on their phone right now, you have higher risk because of, one, you're probably using Wi Fi and in many cases you're going to be using public Wi Fi because it's free and public Wi Fi is easily spoofed. And any of the data that is on a compromised Wi Fi that's sent from your mobile device can be seen and used. Also, you have a ton of apps on the phone. And even within reputable app stores, there are fake apps that people have downloaded, put in personal information and had them scammed. And then, of course, it's a mobile device, and there's

over 800,000 mobile devices that are stolen every year. So, data loss or theft is another reason. So, I recommend if you're going to transact anything that's important, do it at least on an iPad. It's not as mobile, but laptop or desktop are preferred.

>> Okay. We got a really great question over here. Are there any broad trends happening in the world of AI that are positive? [Laughs].

>> Yes.

>> We've been a little negative apparently. [Laughs].

>> In some of the discussions I've had with some reporters this week about predictions, when I go through some of those things that I say, brain hacking or agentic AI is going to replace human error as the number one cause of data breaches, which is another prediction, everybody goes, Mike, you're so doom and gloom. And the fact is that AI also can be used for positive things. And in our list of things, how to protect yourself, you can go ahead and use AI, like ChatGPT, something like that. How do I protect myself? What do I do if this happens? It's a great way to find, not only protection tools but we're using AI on our Experian.com site forward slash data breach, which is another resource to be able to go ahead and have an AI chat bot, and that chat bot can answer questions about how to protect yourself. So, there are some good ways where AI, in fact, is being used not only for preventative tips, consumer tips, and organizations are using AI to be able to protect your data that they hold.

>> Very nice. And Liz had just put the link for you guys in the chat. So, excellent. Are there any other questions today? Any final thoughts then, Mike? [Laughs].

>> My final thought is a little prevention goes such a long way. And if you just take these simple steps to lock your credit file or freeze your credit file, to be able to not click on any links, don't answer any phone calls, those types of things, you don't really need to worry as

much. Because identity theft is also like the old bear chasing people analogy. You don't have to be the fastest person in the group, you just have to be faster than the slowest person in the group. Again, another Experian fact, there's still about 15 to 20 percent of the US population that hasn't taken the precautions like we talked about on the webinar today. And hackers go for the easiest mark, just like a burglar cases a house, and they go after the person that doesn't lock their doors or doesn't have a security system. So take some simple precautions and you'll be much better off. And, of course, if you ever need anything and have any questions, you can always go to Experian.com/databreach, where we have the consumer tips. We also have our 2026 predictions if you're looking for those as well.

>> Fantastic. One other thing that I don't think we mentioned yet, so I will mention it now is, if you are not in the habit of checking your credit reports That's one of the best ways you can find if there has been any activity that you aren't aware of or didn't give permission for, is to check your annual credit reports. You are allowed to do that through annualcreditreport.com. It is free to check your credit reports. It does not impact your credit score. You will not receive your score with your credit reports without paying a small fee, or, at least, unless there are other ways you can get your score for free. But, do get in the habit of checking your credit reports on a regular basis. That'll help you keep tabs on any unauthorized activity, etc. So I think that might be my parting word. So I will say thank you to everyone for being here. Oh wait, we just got another question. Sorry. How can a victim of identity theft correct errors reported to the credit reports due to fraud or scam transactions?

>> I can answer that one.

>> Go ahead, Mike.

>> Yeah. So at any one of the bureaus, all you have to do is contact their customer service line, tell them what you want to do, and an agent will go ahead and tell you what information, whether it's again, back to the point I made about a police report. If you have fraud that's been committed or a scam or anything like that, they'll ask for a copy of the police report or any information. They may ask you for a confirmation or affidavit from the bank or credit card issuer or wherever where that fraud occurred, and then they will be able to clean up and correct the incorrect information on that file, and that's regardless of whether it's Experian or the other two bureaus.

>> Excellent. Thank you. Any other thoughts or questions? I am going to put my email in the chat as well in case anyone needs to reach me or Mike after this is over, but for now you will get a copy of these slides. They will be sent out within the next couple of days or a week, week to two maybe, and the replay will be available. If there's someone who wasn't here today that needs to watch this, that will be available on the FRC website, which again is financialresiliencecenter.org. And let's see, one - gotcha. Says one often needs the identity theft report from identitytheft.gov when correcting their reports. That, I believe, is through the FTC and can be a very useful site. If you are a victim of identity theft, the FTC can walk

>> Yes. you through all the steps of correcting that and making sure you're doing everything you need to. So, yes, identitytheft.gov is a great website. Thank you. All right. Anything else for the good of the order? If not, once again, I will say thank you to Mike for being here today from Experian. Thank you to our ASL interpreters and cart services, our staff behind the scenes answering questions and helping with administration, shall we say. Thank you everyone. And with that, we will say have a great rest of your day.

>> Thanks, Becky.

>> Take care.