

IDENTITY THEFT TODAY

Avoiding Social Security Scams

May 20, 2026
12pm - 1pm EST



SESSION NOTES

Below is a summary of the topics and items discussed in the May 2026 session of **Identity Theft Today: Avoiding Social Security Scams**.

These notes were compiled following a virtual webinar presentation and are provided for general informational purposes only. The session was presented by an attorney licensed in a specific state. Attorneys are not licensed in every state, and laws, regulations, terminology, and requirements vary by jurisdiction. This content is not legal advice and should not be relied upon as such. While best efforts were made to accurately capture the discussion, this document is a transcription summary and may contain errors, omissions, or inaccuracies in wording, facts, or interpretation. Legal Resources and the presenter are not responsible or liable for any consequences that may arise from reading, using, or interpreting this material. For legal advice specific to your situation, please consult with a qualified attorney licensed in your state.

SESSION TOPICS

Scam Overview | Fear and Greed | Red Flags | AI-Powered Scams | Protecting Yourself
Locking Your Identity | Credit Freezes | Reporting Fraud | Key Resources

[Click Here to Access Recorded Session](#) →

SCAM OVERVIEW

- Americans lost nearly \$13 billion to fraud in recent years, with imposter scams ranking as the most frequently reported category. Social Security scams involve criminals impersonating government officials and contacting potential victims by phone, email, or social media. The ultimate goal is to steal money or harvest personal data that can be used for further fraud.

FEAR AND GREED

- Scammers exploit two core emotions to override rational thinking. With fear, they may threaten arrest, claim your Social Security number has been suspended, or warn of asset seizure. With greed, they dangle false promises such as benefit increases or cost-of-living bonuses in exchange for a fee. Urgency is always part of the trap, pressuring targets to act immediately rather than pause and verify.

RED FLAGS

- The Social Security Administration will never threaten you, demand immediate payment, suspend your Social Security number, request credit card or bank information over the phone, ask for payment via gift cards or cryptocurrency, or promise new benefits for a fee. Any legitimate cost-of-living adjustments are applied automatically and free of charge. If any caller makes these demands, it is a scam.

AI-POWERED SCAMS

- Criminals are leveraging artificial intelligence to make scams harder to detect. Deepfake voice technology allows callers to sound exactly like a government official. Caller ID spoofing makes incoming calls appear to come from a legitimate Social Security number, and scammers may even reference a real employee's name and badge number sourced from LinkedIn. Fraudulent social media accounts and phishing emails further expand their reach. If you receive a suspicious email, never click any link; instead, contact the agency directly to verify its legitimacy.



PROTECTING YOURSELF

- The simplest defense is to hang up and ignore suspicious calls, texts, or emails. Never share your Social Security number, bank account, or credit card information with an unexpected caller. If you believe a call might be legitimate, hang up and call the Social Security Administration directly at 1-800-772-1213 or log in at SSA.gov. Creating an official My Social Security account online is strongly recommended, as it prevents criminals from setting one up in your name.

LOCKING YOUR IDENTITY

- The E-Verify Self Lock tool allows you to place a lock on your Social Security number that prevents anyone from using it for unauthorized employment. This is separate from a credit freeze and specifically addresses employment-related identity fraud and unemployment fraud. While the lock is active, any employer verification will return a tentative non-confirmation. You can temporarily lift the lock whenever you need it for legitimate employment purposes, then re-engage it immediately after.

CREDIT FREEZES

- A credit freeze, placed with all three major bureaus (Equifax, Experian, and TransUnion), blocks anyone from accessing your credit report to open new accounts. Unlike a fraud alert, which simply flags your file and relies on lenders to follow through, a credit freeze provides a hard block. It is free to place and can be temporarily lifted for 24, 48, or 72 hours when you need to apply for credit, then reactivated immediately. Freezes can be managed online or by phone with each bureau.

REPORTING FRAUD

- If you suspect fraud or discover suspicious activity, act quickly. File a complaint with the SSA Office of the Inspector General, report identity theft at ReportFraud.FTC.gov, and visit IdentityTheft.gov for personalized step-by-step recovery plans. Keep copies of all reports, letters, and confirmation numbers. Reporting helps law enforcement identify patterns and track criminal networks. Contact your identity theft protection provider right away to begin resolution and recovery support.

KEY RESOURCES

- SSA Direct Line: 1-800-772-1213
- SSA.gov – Create a My Social Security account and review benefits
- ReportFraud.FTC.gov – Report fraud and identity theft to the FTC
- IdentityTheft.gov – Recovery plans and identity protection guidance
- E-Verify.gov – Self Lock tool to prevent employment fraud

Q&A HIGHLIGHTS

Q1. What should I do if I get an alert that my Social Security number was found on the dark web?

A: A dark web alert means your information has been detected but does not necessarily mean someone is actively using it. Take precautions immediately by placing a credit freeze with all three credit bureaus. A credit freeze provides stronger protection than a fraud alert because it blocks access entirely, whereas a fraud alert only adds a note to your file that lenders may choose to ignore.

Q2. Does the E-Verify lock help if someone tries to file a fake IRS tax return in my name?

A: No. The E-Verify Self Lock is specifically designed to prevent unauthorized employment verification and is not the same as an IRS identity protection PIN. For tax-related fraud, the IRS offers a separate Identity Protection PIN that you can set up directly through the IRS to prevent fraudulent tax filings.

Q3. Are only older people targeted by Social Security scams?

A: Older adults are disproportionately targeted because many rely heavily on Social Security benefits, making them more susceptible to fear-based tactics. However, anyone can be a target. Younger individuals may be somewhat less vulnerable due to greater familiarity with technology and a tendency to question unsolicited contact, but no age group is immune.

Q4. Is it safe to give out the last four digits of my Social Security number?

A: If a legitimate, verified company requests the last four digits for identity verification, it is generally acceptable. However, if you receive an unexpected call asking for this information, hang up and call the company back at their official number to confirm they initiated the request. If you are uncomfortable, ask if there is an alternative verification method available.

Q5. My mother passed away last year. Should I contact all three credit bureaus?

A: Yes. Reach out to Equifax, Experian, and TransUnion to freeze your late mother's credit if it has not already been done. In many cases, the funeral home handles this notification, so check with them first. Freezing the credit of a deceased family member prevents criminals from opening accounts or taking out loans using their personal information.

ABOUT THE SPEAKERS



EUGENE NAKOUYE

IRIS IDENTITY THEFT PROTECTION

Operations Manager at IRIS Identity Theft Protection with 13 years of experience. Holds a cybersecurity certification and oversees the resolution team, serving as a resource for members navigating identity theft prevention and recovery.

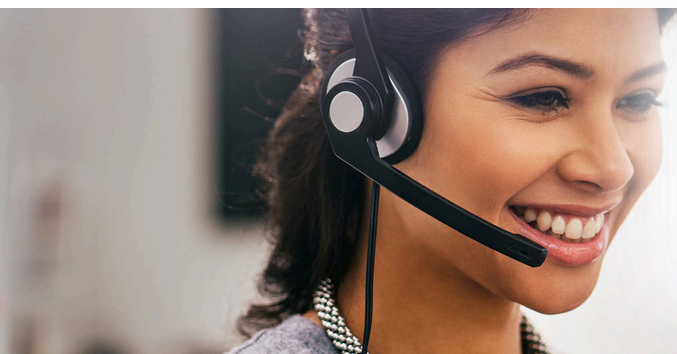


TIARA EPPS

IRIS IDENTITY THEFT PROTECTION

Supervisor of Operations at IRIS Identity Theft Protection with 14 years of experience. Began as a Resolution Specialist Agent and advanced through the organization, now leading a team focused on guiding members through identity theft resolution and protection.

DISCLAIMER: This summary highlights key webinar points and questions. For comprehensive details, view the full seminar at [LRSeminars.com](https://www.LRSeminars.com).



Contact Us

Our Member Services team is available for assistance.

Phone: 800.728.5768
Email: info@legalresources.com

www.legalresources.com