

Identity Theft: Prevention, Detection and Resolution

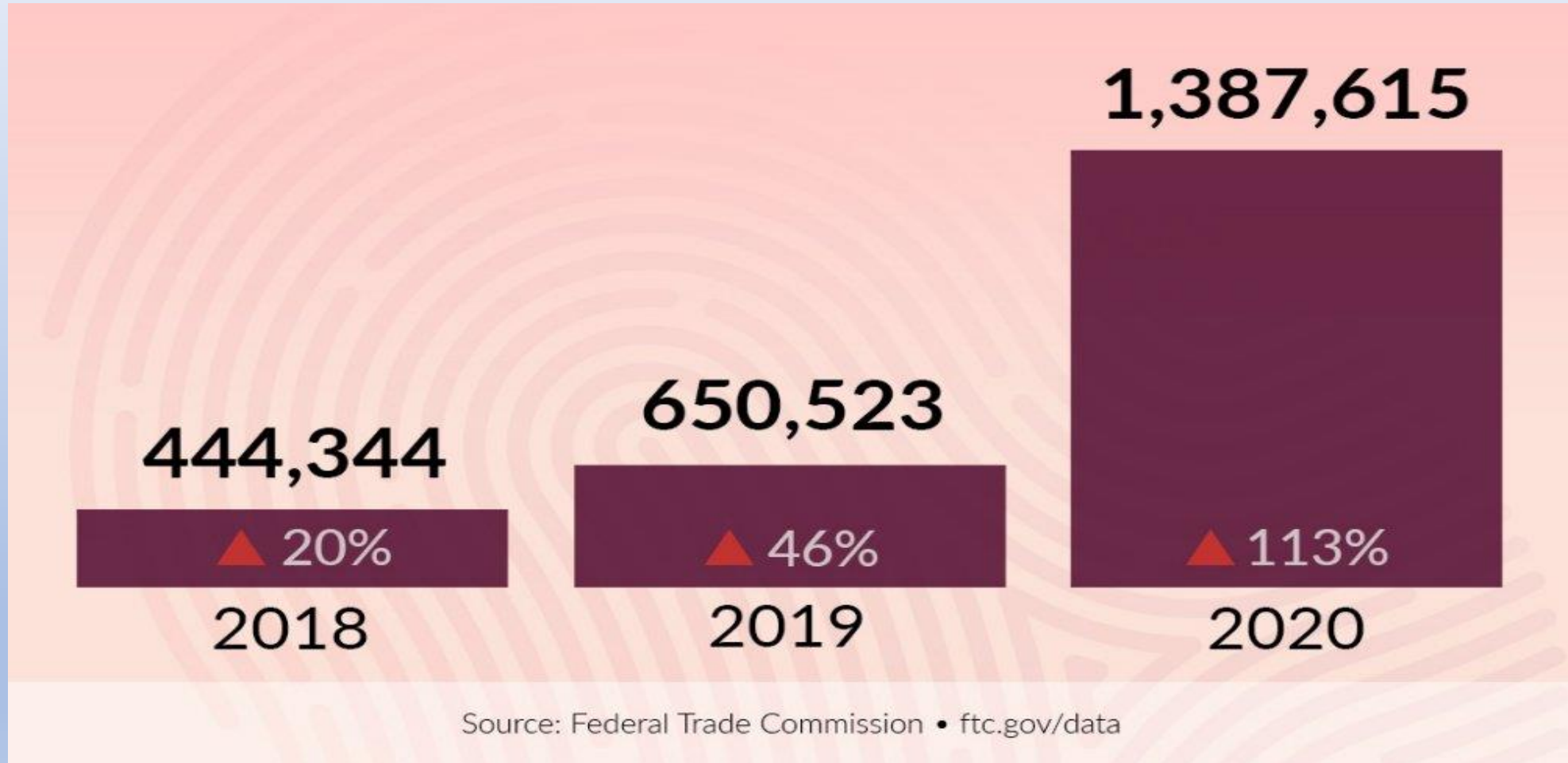
brought to you by NYSUT Member Benefits

Martin Lynch: Director of Education and Compliance Manager, Cambridge Credit Counseling

Derek Clement: CFP, NYSUT Member Benefits

This presentation should not be interpreted as legal advice. It is intended for educational purposes only.

Identity theft is increasing



True identity theft involves the opening of new accounts.

- Data breaches expose your identity, but your information may not be used – at least not immediately. Your info may be sold on the dark web to the actual criminals who will then use your identity.
- People with poor credit are also victims. The lower the victim's credit rating, the less their identity will cost.
- Identity theft comes in many forms: bank fraud, credit card fraud, utility fraud, loan or lease fraud, employment or tax fraud.

COVID relief has become a target

- According to the Department of Labor, at least \$36 billion of the \$360 billion in CARES Act unemployment benefits was lost to improper payments, mostly from fraud, *by last November*.
- Criminals go where the opportunity is greatest, and where the chances of being caught are least.
- The chances of being caught buying identities on the dark web are minimal.
- From data breaches to dumpster diving, from installing “skimmers” at payment terminals to accessing your computer over public wi-fi, criminals use many methods to steal access to your information.

Detection - Indicators

- You find unfamiliar accounts or charges on your credit report. Get your reports for free until April 2022 at www.annualcreditreport.com. Get your free Chex Systems report at [Home \(chexsystems.com\)](http://Home(chexsystems.com)).
- Unexplained withdrawals from your bank account. Get your free Chex Systems report at [Home \(chexsystems.com\)](http://Home(chexsystems.com)).
- You get bills for items you didn't order or statements for credit cards you didn't sign up for. You don't receive all of your bills or other mail.
- Medical providers bill you for services you didn't use.
- Your credit score drops significantly. You're refused credit.
- Debt collectors call you about debts you don't recognize.

Detection - Indicators

- Your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit or won't cover you because your medical records show a condition you don't have.
- The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you don't work for, or that you've already been sent a refund.
- You apply for unemployment compensation and are informed you're already receiving it, or you receive a letter from your state indicating your application has been denied.
- You get notice that your information was compromised by a data breach at a company where you do business or have an account.

Resolution

- Get all 3 credit reports to identify as many bogus accounts as you can. (Reporting is voluntary, so the fraudulent accounts may not appear.)
- Assemble statements on fraudulent accounts.
- Start a notebook to document every step taken, including every creditor with whom you've spoken, the time/date/content of each call, etc.
- Contact creditors, letting them know you're an ID theft victim. If they ask you to make payments on fraudulent accounts/charges, refuse to do so. Close fraudulent accounts.
- Consider freezing your credit by contacting credit bureaus. You can do this online.

Resolution

- File a local police report, even if the theft occurred online. Make many copies of the police report to distribute to creditors/collectors. Always keep the original report.
- File a federal report at www.identitytheft.gov. Make copies.
- Check with registry of motor vehicles to ensure a bogus license wasn't issued.
- Check with U.S. State Department to ensure that passport wasn't issued.
- Check with local post office to ensure change of address form wasn't filed.

Resolution

- **Contact the Social Security Administration (SSA).** In an extreme case, you may be able to change your Social Security number, but it is difficult to do and may not resolve the problem.
- **Change your PINs.** If your ATM or debit card was stolen, do not use your old PIN for your new card.
- **Stop payment on checks.**
- **Deal with debt collectors.** Inform the collector by phone and in writing that you are a victim of identity theft. In your letter, be sure to include copies of documents, such as a police report, that demonstrate that you're the victim of identity theft. Do not make "good-faith" payments toward debt.

Resolution

- Ask the collector to provide you with all pertinent information (for example, name, phone number, address, account number) relating to both the collector and creditor.
- Ask the collector to confirm in writing that you are not responsible for the outstanding debt and that the collection account has been closed.
- If the collector continues collection efforts or you receive a notice of additional legal action, consult an attorney immediately.

Prevention

1. **Freeze your credit – a free option** all three major credit bureaus — Equifax, Experian and TransUnion — restricts access to your records so new credit lines can't be opened. It's free to freeze your credit and unfreeze when you want to open an account.
2. **Avoid providing your SSN.** Ask why it's needed and if they'll consider alternative methods of verifying your identity. Never carry your Social Security card with you. Shred documents that include your SSN.
3. **Avoid using public Wi-Fi.**
4. **When online:** Consider using a private search engine and/or VPN (virtual private network) and only submit financial info through HTTPS sites. Use strong, unique passwords that can't be deduced from social media content.
5. **Monitor your credit reports/scores regularly.**
6. **Shred account statements/documents you don't need.** Don't just throw them in the trash.
7. **Lock your mobile device!** Fewer than half of cell phone owners do this.
8. **Monitor your mail and read your financial statements.**
9. **Consider a service to lock down your identity and monitor the dark web.** They can't prevent identity theft or data breaches, but their monitoring services can be very useful.
10. **Consider using a password manager.** There is a small cost, but these services can be quite sophisticated.

Resolving Unemployment Benefit Fraud

- Report the fraud to the unemployment insurance agency in the state that issued the benefits. <https://webapps.labor.ny.gov/dews/ui/fraud/report-fraud.shtm>
- If possible, report the fraud online. An online report will save you time and be easier for the agency to process.
 - Keep any confirmation or case number you get. If you speak with anyone, keep a record of who you spoke with and when.
 - Follow the steps the agency tells you to take.
- Report the fraud to your employer. Keep a copy of any confirmation you get.
- Report the fraud to the U.S. Department of Justice's National Center for Disaster Fraud (NCDF) by completing an [NCDF Complaint Form](#) online, or by calling 866-720-5721.

Resolving Unemployment Benefit Fraud

- **When you file your income taxes, ONLY include income you actually received.** Do not wait to receive a corrected 1099-G to file your taxes. The processing of your tax return should not be delayed while your report of unemployment identity theft is under investigation.
- If you have not filed your taxes yet, do not report the incorrect 1099-G income on your tax return.
- If you have already filed your taxes, do not file an amended return. The IRS will issue additional guidance regarding your next steps. Refer to the [Identity Theft and Unemployment Benefits](#) page on IRS.gov for updates and additional tax filing information.

NYSUT Resources

- AFT has partnered with CLC ID Protect to provide free coverage for all active and retired members. [Identity Theft Protection | American Federation of Teachers \(aft.org\)](#) **Program includes:**
- Assisted recovery for victims of identity theft
- Up to \$10,000 expense reimbursement coverage
- Free ID Threat Score
- Free Safe Wallet
- **Register Here:** <https://www.clcidprotect.net/co/home/aft/>
- Discounted pricing for additional services
- Questions? Call CLC ID Protect @ (866) 875-8385

NYSUT Member Benefits Resources

- **MetLife Auto and Home** policyholders and **Synchrony Bank** account holders have access to one-on-one support to help resolve Identity Theft through Cyberscout.
 - Personalized response from fraud and breach experts 24/7
 - Industry leading fraud experts with an average of 9 years of experience
 - On-call bilingual resolution experts
 - 866.305.7216 or cyberscout-idtheft.com
 - More info on our endorsed **MetLife Auto and Home** Insurance and the **Synchrony Savings Bank Program** visit memberbenefits.nysut.org
- **Legal Service Plan**
 - Victims of identity theft will be given comprehensive advice and guidance on how best to proceed to reclaim their identity. In limited circumstances may include the writing of up to three letters per plan year
- **Cambridge Credit Counseling**

Resources

- **Federal Trade Commission:** To report identity theft: <http://www.identitytheft.gov> : 1-877-438-4338;1-866-653-4261 (TTY)
- **U.S. Postal Inspection Service:** To file a complaint: <https://www.uspis.gov/report/> 1-877-876-2455
- **IRS:** <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft>; 1-800-908-4490
- **Social Security Administration:** To report fraud: go to <http://www.socialsecurity.gov> and type "Fraud" in the Search box.
SSA by phone: 1-800-269-0271; 1-866-501-2101 (TTY)

Resources

- **U.S. Postal Service:** To place a hold on mail; <http://www.usps.com/holdmail>
- **U.S. Department of State:** To report a lost or stolen passport:
<http://www.travel.state.gov/passport>; 1-877-487-2778; 1-888-874-7793 (TTY)
- **Bank of America:** <https://www.bankofamerica.com/privacy/resolve-identity-theft.go>; 1-800-432-1000
- **Chase:** <https://www.chase.com/resources/report-fraud>; 1-800-432-3117
- **Capital One:** <https://www.capitalone.com/identity-protection/commitment>; 1-800-227-4825

Resources

- **American Express:** <http://www.americanexpress.com/us/content/fraud-protection-center/what-you-can-do.html>; 1-800-528-4800
- **Discover:** <https://www.discover.com/credit-cards/help-center/faqs/fraud.html> ; 1-800-347-2683
- **Synchrony Bank:** <https://www.mysynchrony.com/account/protect-your-information.html>; 1-866-226-5638
- **Citibank:** <https://online.citi.com/US/ag/contactus>; 1-800-374-9700
- **Wells Fargo:** <https://wellsfargo.com/privacy-security/fraud/report/identity-theft/>; 1-800-869-3557

Resources

Major check verification companies:

- Certegy Check Services, Inc. (800.437.5120)
- TeleCheck (800.366.2425)
- Chex Systems: This is a specialized credit reporting agency that compiles reports about checking and savings accounts. Monitoring your chexsystems report can indicate whether new bank accounts have been opened in your name. You're entitled to one free report per year.
- [Home \(chexsystems.com\)](https://www.chexsystems.com)

NYSUT Member Benefits Resources

Cambridge Credit Counseling

- Free one-on-one debt consultation with a certified counselor
- Student Loan Solutions: 888-254-9827
 - memberbenefits.nysut.org/student-loan-center
 - Public service loan forgiveness
 - Teacher loan forgiveness
 - Income-based repayment plans
 - Student loan portal – full report for only \$14.95
- Debt Management/Credit Card Debt Consolidation: 888-254-0398
 - memberbenefits.nysut.org/program-service/legal-and-financial/debt-counseling
- Foreclosure Intervention
- Reverse Mortgage Counseling
- First Time Homebuyer Assistance Education
- Bankruptcy Counseling