



Safeguarding Your Identity



Important disclosures

This event is for informational purposes only and is not meant as investment advice or a recommendation to engage in any investment strategy. Investment decisions should always be made based on your specific financial needs, objectives, goals, time horizon and risk tolerance. Securities discussed may not be suitable for all investors.

IVY INVESTMENTSSM refers to the investment management and investment advisory services offered by Ivy Investment Management Company, the financial services offered by Ivy Distributors, Inc., a FINRA member broker dealer and the distributor of IVY FUNDS[®] mutual funds and IVY VARIABLE INSURANCE PORTFOLIOS[®], and the financial services offered by their affiliates.

NOT FDIC/NCUA INSURED | MAY LOSE VALUE | NO BANK GUARANTEE NOT A DEPOSIT | NOT INSURED BY ANY FEDERAL GOVERNMENT AGENCY

What is Identity Theft?



Impact of identity theft

- 16.7 million U.S. consumers are victims of identity fraud
- An increased by 8%
- \$16.8 billion in financial losses

Source: 2018 Identity Fraud: Fraud Enters a New Era of Complexity, Javelin Strategy & Research.

Your identity includes

- Name
- Address
- Date of birth
- Bank account number
- Mother's maiden name
- Social Security number
- Passwords

How thieves get your information

- Data breaches
- Card skimmers
- Fake Wi-Fi hotspot
- Phishing
- Physical theft

What can thieves do with your identity?

- Open new financial accounts
- Obtain medical care
- Falsify tax returns to obtain refunds
- Open new utility accounts
- File for Social Security benefits in your name

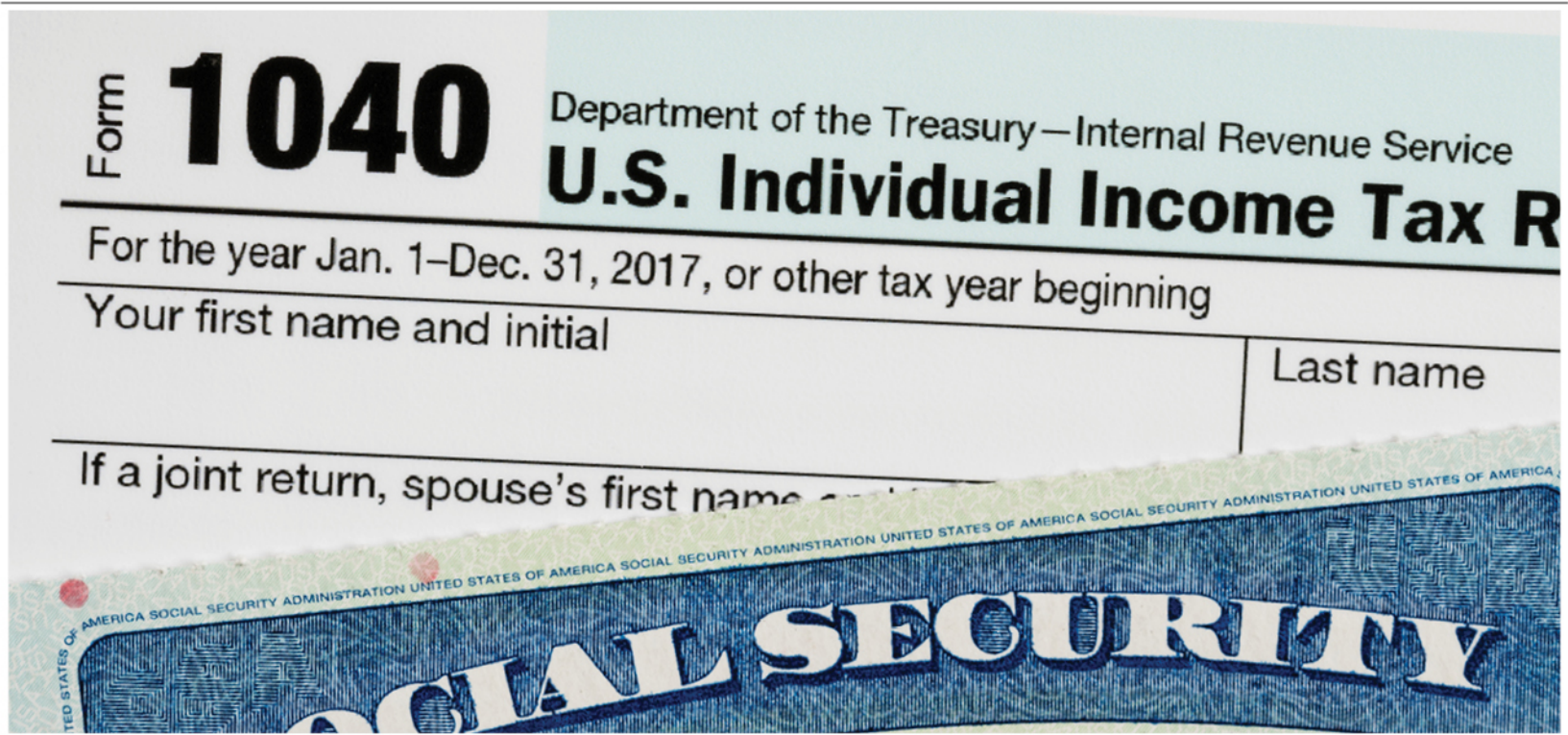
Identity Fraud



CitiBank Card Solutions is used in this presentation under the Standard YouTube License.
The trademarks and other intellectual property depicted therein are those of their respective owners

SAFEGUARDING YOUR IDENTITY

Tax refund fraud



Cell phone hijacking



Child identity theft



Medical identity theft



Five Ways to Avoid Identity Theft



Protect your Social Security number

BEFORE YOU GIVE OUT YOUR SOCIAL SECURITY NUMBER, ASK THESE QUESTIONS:

- Why do you need my number?
- What law requires its use?
- How will it be used?
- What will happen if I refuse?

Protect yourself in your home

- Store personal information, statements and other papers in a secure place.
- Collect the mail every day.
- Pay attention to your billing cycles.
- Purchase and use a shredder.

Protect yourself on your phone

- Use the security features on your phone.
- Update sharing and firewall settings when you're on a public Wi-Fi network.
- Be wary of shoulder surfing.
- Establish a PIN or password with your mobile carrier.

Protect yourself on your computer

- Look for “https” in any web address where you send personal information.
- Practice safe email protocol.
- Keep operating systems and software up to date.
- Always think before you share.

Protect your medical identity

- Guard your insurance card as you do your credit cards.
- Give your information only to the medical professionals you know.
- Shred all medical documents, including prescriptions.
- Monitor all medical billing statements.

Help, I May Have Been Hacked!



Early warning signs of fraud

- You don't get your bills or other mail.
- You receive calls about debts that aren't yours.
- You find unfamiliar charges on your accounts.
- Your health plan rejects a medical claim because you've reached your benefit limit.
- The IRS notifies you that more than one tax return has been filed in your name.
- An unexpected drop in your credit score.

Be proactive

- Under federal law you are entitled to a copy of your credit report.
- You can obtain one credit report each year from:
 - » Experian
 - » Equifax
 - » TransUnion
 - » Innovis
- Check your credit report from each agency annually.

What to do if fraud has occurred

- Call the companies where you know fraud occurred.
- Order all four credit reports and examine them for new accounts that have been opened.
- Report identity theft to the Federal Trade Commission (1-877-IDTHEFT).

Begin to repair the damage

- Close new accounts opened in your name.
- Remove fraudulent charges from your accounts.
- Correct your credit report.
- Freeze your credit.

Credit report freezing

- Prevents many types of accounts from being opened.
- Contact the bureau to lift the freeze when needed.
- You can freeze a child's account.
- Freezes and lifts are free.

You may need to consider additional steps

- Report a misused Social Security number.
- Stop debt collectors from trying to collect debts you don't owe.
- Replace government-issued IDs.
- Clear your name of criminal charges.



Safeguarding Your Identity

