



# PREVENTING & RESPONDING TO IDENTITY THEFT



**May 2014**

**New York Department of State  
Division of Consumer Protection**

[www.dos.ny.gov](http://www.dos.ny.gov)

# New York Department of State's Division of Consumer Protection

---

- Protect New Yorkers by publicizing unscrupulous and questionable business practices and product recalls
- Conduct investigations and hearings
- Enforce the “Do Not Call Law”
- Research issues
- Develop legislation
- Create consumer education programs and materials
- Respond to individual marketplace complaints by mediating and securing voluntary agreements
- Represent the interests of consumers before the Public Service Commission (PSC) and other State and federal agencies

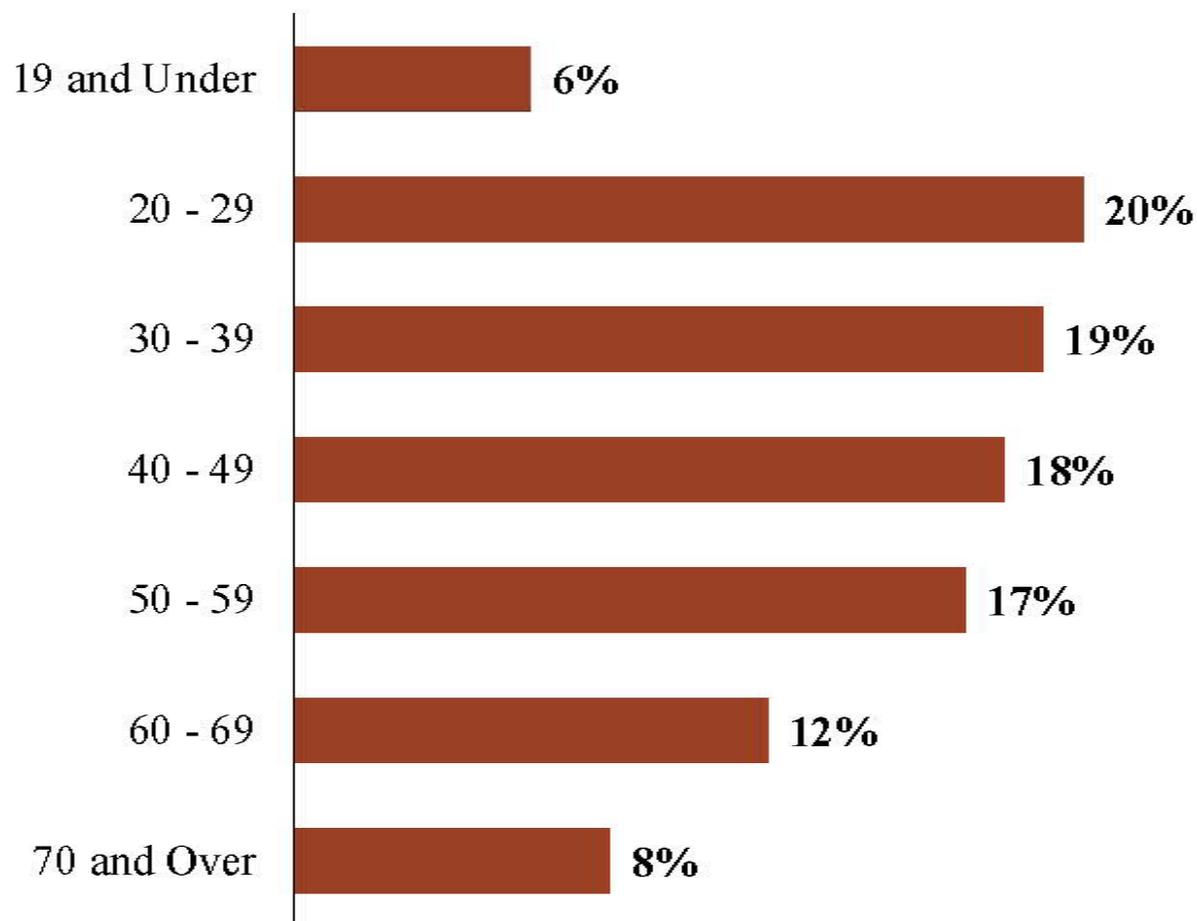
# Identity Theft

---

- The practice of stealing someone's personal information with the intent to fraudulently obtain goods, property, credit, utility services, employment or government documents
- Where the use of stolen identifying information is provided to law enforcement by the imposter during a criminal investigation, traffic stop or upon arrest
- Some versions:
  - “New Credit Account”
  - “Account Takeover”
  - Criminal Identity Theft

# Consumer Sentinel Network Identity Theft Complaints by Victims' Age<sup>1</sup>

*January 1 – December 31, 2013*



**Consumer Fraud and Identity Theft Complaint Data for 2013, FTC 2014**

**Preventing and Responding to Identity Theft**

New York Department of State's Division of Consumer Protection

# The Incidence of Identity Theft

---

- Identity theft was the No. 1 consumer complaint nationwide to the Federal Trade Commission
- NYS had the ninth highest per capita identity theft rate in the U.S., with more than 86.9 complaints for every 100,000 residents
- In 2013, the FTC received more than 17,000 identity theft complaints from NYS residents

*Consumer Fraud and Identity Theft Complaint Data for 2013, FTC, 2014*

## Identity Theft Complaints Count from New York Victims = 17,072

### *Identity Theft Types Reported by New York Victims*

Rank	Identity Theft Type	Complaints	Percentage <sup>1</sup>
1	Government Documents or Benefits Fraud	4,979	29%
2	Credit Card Fraud	3,587	21%
3	Phone or Utilities Fraud	2,201	13%
4	Bank Fraud	1,693	10%
5	Employment-Related Fraud	644	4%
6	Loan Fraud	583	3%
	Other	3,746	22%
	Attempted Identity Theft	1,486	9%

<sup>1</sup>Percentages are based on the 17,072 victims reporting from New York. Note that CSN identity theft complaints may be coded under multiple theft types.

*Consumer Fraud and Identity Theft Complaint Data for 2013, FTC 2014*

## Preventing and Responding to Identity Theft

New York Department of State's Division of Consumer Protection

# The Dollar Cost

---



- In 2013, consumers reported losses from fraud and identity theft of more than \$1.6 billion
- The median monetary loss from fraud was \$400 per person

*Consumer Fraud and Identity Theft Complaint Data for 2013, FTC 2014*

# Types of Identity Theft

---



- Financial Identity Theft most common form of identity theft
- Criminal Identity Theft
- Medical Identity Theft
- Employment Identity Theft
- Government Document/Benefits Fraud
- Synthetic Identity Theft
- Fraudulent IRS Tax Returns

# Warning Signs of Identity Theft

---

- Receipt of bills for purchases never made
- Denial of credit for no apparent reason
- Cessation of monthly bank or credit card statements
- Inaccuracy of credit report information
- Contact by creditors, debt collection agencies and law enforcement
- With respect to **child identity theft**: your child receives offers for credit or credit cards in the mail

# How to Prevent Identity Theft

## Overview

---

- Check your financial statements promptly. Time is critical!
- Get your credit report **FREE** every four months (you can get a free report from each of the three major credit bureaus once a year, for a total of three free reports annually)
  - If you are a victim of identity theft, you are entitled to at least one additional free report
- Shred documents containing personal information, especially your Social Security number, by using a cross-cutter shredder
- Sign credit card, not by name, but by asking for proof of identity (for example, “Please See Driver’s License”)

# How to Prevent Identity Theft

## Overview

---

- Opt out from receiving unsolicited offers of credit by calling **888-5-OPTOUT**
- Travel light -- the less personal information you carry around, the less you can potentially lose
- Secure your mail
- Be wary of “shoulder surfing” and other attempts to obtain your personal information while shopping and/or using an ATM
- Protect your personal data, such as your Social Security number -- be stingy when giving it out!

# How to Prevent Identity Theft

## Guarding Your Social Security Number

---

- When an entity requests your number, inquire as to how and why the number is used, and ask for an alternative
- In most cases in New York, businesses cannot:
  - Post or display publicly a Social Security number
  - Require you to transmit your Social Security number over the Internet unless the connection is secure or encrypted
  - Require you to log onto the web using your Social Security number without a password
  - Print your Social Security number on materials mailed to customers
- Public or private elementary or secondary schools and colleges may not use social security numbers as student identifiers (Ed. Law 2-b)

# How to Prevent Identity Theft

## Protect Online Financial Transactions

---

- Use secure connection: https will start the web address
- Depending upon which browser you use, a **secure** connection will make your browser display a **closed lock** or an **unbroken key symbol** in the lower portion of your window (vs. an open lock or a broken key for non-secure connections)

# How to Prevent Identity Theft

## When Communicating Online

---

- Do not fall for online scams, such as phishing, that attempt to steal your assets and identity
- Install spam filters or settings to help reduce junk mail
- Beware of spyware
- Only transmit sensitive data through encrypted sites
- Exercise caution when connecting via wireless

# If You Are a Victim of Identity Theft

## Steps You Can Take

---

Where appropriate:

- File a police report. Ask for a copy and keep it in a secure place for use with creditors and to get consumer transaction records
- Notify all banks, creditors, utilities, insurance carriers, phone, Internet service and cable television providers, libraries, and other memberships
- Close bank and credit card accounts; request new PINs and account numbers
- Alert credit reporting agencies -- place a **Security Freeze** or **Fraud Alert** on your credit report
- Request a **FREE** credit report to check for discrepancies

# If You Are a Victim of Identity Theft

## Steps to Take

---

Where appropriate:

- You may notify credit reporting agencies of incorrect information and request correction by mail, telephone or via e-mail. If necessary, follow up to confirm delivery of your corrections
  - Check up on the removal, and be persistent, as credit agencies sometimes fail to remove incorrect information even after request has been made
- Contact secondary credit bureaus, including check approval agencies
- Request your earnings statement from the Social Security Administration
- Check with the U.S. Postal Service to investigate whether an identity thief has set up a fraudulent address under your name

# If You Are a Victim of Identity Theft

## Steps to Take

---

Where appropriate:

- Contact the U.S. State Department if your passport was stolen. If the passport was issued by another country, contact the issuing country's consulate or embassy
- Notify the U.S. Secret Service if the crime involved hacking into computers or counterfeit credit cards
- File a report with and other necessary FTC documentation (for example, an affidavit):
  - At [www.FTC.gov](http://www.FTC.gov) or
  - Call the FTC Hotline at 1-877-IDTHEFT
- Notify the State Department of Motor Vehicles

# Security Breach and Identity Theft

---



- A security breach occurs when there is unauthorized access to your private information held in electronic format by an entity, such as a business or government agency
- Can result in someone using your personal information to make fraudulent purchases or transactions
- Under NYS law, persons and companies conducting business in NYS are required to notify residents of the unauthorized access to private computerized information

# Security Breach

## Steps to Take if Your Personal Information is Lost or Stolen From a Business

---



- **Get the facts from the notification**
- **Take identity theft precautions**
- **Watch for signs of fraud**
- **Ask if the credit reporting agencies were notified**

# Security Breach

## Steps to Take if Your Personal Information is Lost or Stolen From a Business

---



- **Check your credit report**
- **Consider closing affected accounts**
- **Learn more about personal information protections, such as security freeze or a fraud alert from the CPB**
- **Retain your paperwork**

# The State's Identity Theft Resource

---

- The New York Department of State's Division of Consumer Protection's consumer advisors can act as liaisons to intervene and troubleshoot for consumers to help victims recover from the damages of identity theft
  - Including with creditors, financial institutions, credit-reporting agencies, State and other governmental agencies, utilities companies and employers
- The Division hosts new and updated identity theft-related information to assist consumers and liaisons and provide free mediation services

# The State's Identity Theft Resource

---

- An elderly or disabled identity theft victim may be eligible for financial compensation if s/he satisfies requirements
  - Out-of-pocket expenses for financial counseling in connection with the identity theft may be reimbursed
- State residents who are victims of identity theft may be eligible for financial restitution for costs, actual losses and consequential losses incurred due to offender's criminal conduct
  - This *may* also include financial restitution for time spent repairing victims' credit standing due to identity theft
- The Division, in conjunction with victim service providers, are offering new tools to help consumers track and determine the number of hours and the value of the time used to repair their credit standing due to identity theft
- A victim of identity theft should keep a "compensation journal" containing detailed records and receipts of all expenses incurred in rectifying the identity theft and re-claiming his/her good name. This journal can be submitted for a restitution award in court if the case is prosecuted
- To learn more, visit the website at [www.cvb.state.ny.us](http://www.cvb.state.ny.us) or call 800-247-8035

# The State's Identity Theft Resource

---

- Identity Theft -- A Consumer's Guide
- New York State Security Freeze

# Summary

## Identity Theft Safety Tips

---

- Watch for warning signs of identity theft
- Know how perpetrators steal personal information, and guard your and your children's personal information
- Take appropriate steps to clear your name and prevent further damage if you suspect that you could be, or if you are, a victim of identity theft
- Quick action limits loss from an identity thief's actions in your name

# Summary

## Identity Theft Safety Tips

(cont'd)

---

- Know your rights with respect to credit reporting agencies
- Exercise caution when using an ATM
- Pursue your rights under NYS law in the event of a security breach
- Explore restitution if you have been victimized

# Questions?

---



**New York Department of State  
Division of Consumer Protection**

**[www.dos.ny.gov](http://www.dos.ny.gov)**

***Advocating for and Empowering  
NY Consumers***

**1-800-697-1220**

**Thank You**



# PREVENTING & RESPONDING TO IDENTITY THEFT



**May 2014**

**New York Department of State  
Division of Consumer Protection**

**[www.dos.ny.gov](http://www.dos.ny.gov)**