The Increasing Threat of Identity Theft

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller

MAY 2021

Message from the Comptroller

May 2021

The era of COVID-19 has brought enormous suffering and persistent uncertainty to New Yorkers. Adding to both the financial and psychological pain of the pandemic is a dramatic increase in identity theft during the past year.

More than 67,000 complaints of identity theft were reported in New York State during 2020, according to the Federal Trade Commission (FTC). That was a record number, up 85 percent from the previous year and more than four times the figure of a decade earlier.

Whether identity theft involves credit cards, bank accounts, business or personal loans, government benefits or other types of transactions, it carries significant risk of financial loss to the victim. The U.S. Department of Justice reported $15.1 billion in financial losses nationwide in 2018. Even when there is no direct monetary loss, addressing the consequences of stolen personal information can take months of complicated work with banks, utility companies, medical offices and others. Sometimes the worst damage comes later, when victims have trouble getting a job, renting an apartment, obtaining a tax benefit or receiving a loan because of a stolen identity.

New York State has taken numerous steps in recent years to address identity theft, which is punishable by up to seven years in prison, and to require that businesses and State agencies safeguard private personal information. But clearly, more must be done.

Each of us can and should take common-sense steps such as making sure to keep Social Security numbers confidential, and being careful to limit use of birth dates and other personal information in online communications—including social media. Governmental and independent consumer advocates offer a number of other recommendations for individuals, which are detailed in this report.

As policy makers at all levels of government consider additional responses to identity theft, private businesses large and small that collect and maintain personal information must redouble their efforts to safeguard such data. Social media companies, whose business models rely heavily on personal information, should take steps to promote best practices, such as educating users about ways to keep private information confidential.

Working together, we can reverse the rising tide of identity theft.

Thomas P. DiNapoli
State Comptroller

Contents

Executive Summary

Identity theft cases surged in New York State in 2020, inflicting financial losses on individuals and threatening disruption to government programs as well as private financial institutions. Identity theft complaints surpassed 67,000 statewide last year, more than four times the annual total from a decade earlier, according to Federal Trade Commission (FTC) data.

Credit card fraud was the most frequently reported type of identity theft in the State, with nearly 25,000 New Yorkers reporting their information had been misused on an existing credit card account or to open a new account.

During 2020, more than 3,600 identity theft reports related to COVID-19 were reported in the State, with two-thirds of those related to unemployment insurance or other government benefit programs, according to the FTC. Identity thieves also used individuals' personally identifiable information for a variety of other purposes, including fraudulently obtaining medical services, prescription drugs or medical insurance coverage.

Across the nation, about 70 percent of identity theft victims suffered financial losses, which totaled $15.1 billion in 2018, with average losses of $640 per person, according to the U.S. Department of Justice. With New York representing roughly 5 percent of identity theft reports nationwide, costs to New Yorkers likely total hundreds of millions of dollars annually.

Aside from the immediate financial cost and disruption to daily life, identity theft can affect a victim's ability to get a job, rent an apartment or obtain college loans. In some cases, thieves prey on children by using illegally obtained Social Security numbers for fraudulent purposes that may have damaging longer-term impacts if the crime is not discovered, according to industry experts.

Most reports of identity theft do not end in arrests and convictions. Statewide, identity theft arrests averaged about 750 each year over the past decade, while courts reported an average of 450 convictions and sentencings annually, according to the State's Division of Criminal Justice Services.

New York State laws and regulations impose penalties of up to seven years in prison for identity theft crimes, and require certain businesses to take steps to guard Social Security numbers, credit card accounts and other personal data that is used in such crimes. In addition, the State has established programs to help New Yorkers avoid and recover from identity theft. Authorities in New York and at the national level have levied multi-million-dollar fines on companies that have suffered large data breaches exposing the personal information of individuals. Still, increasing use of personal data online, continuing reports of major data breaches, and dramatic increases in reported cases of identity theft make clear that further steps are needed.

Federal and State agencies, along with independent consumer advocacy organizations, urge individuals to aggressively safeguard Social Security numbers, credit card and bank account numbers, birthdates and other personal private information that can be used in identity theft. More detailed discussion of such steps appears later in this report.

Both in Washington and in Albany, policy makers should take steps to protect personal data and address the growing problem of identity theft.

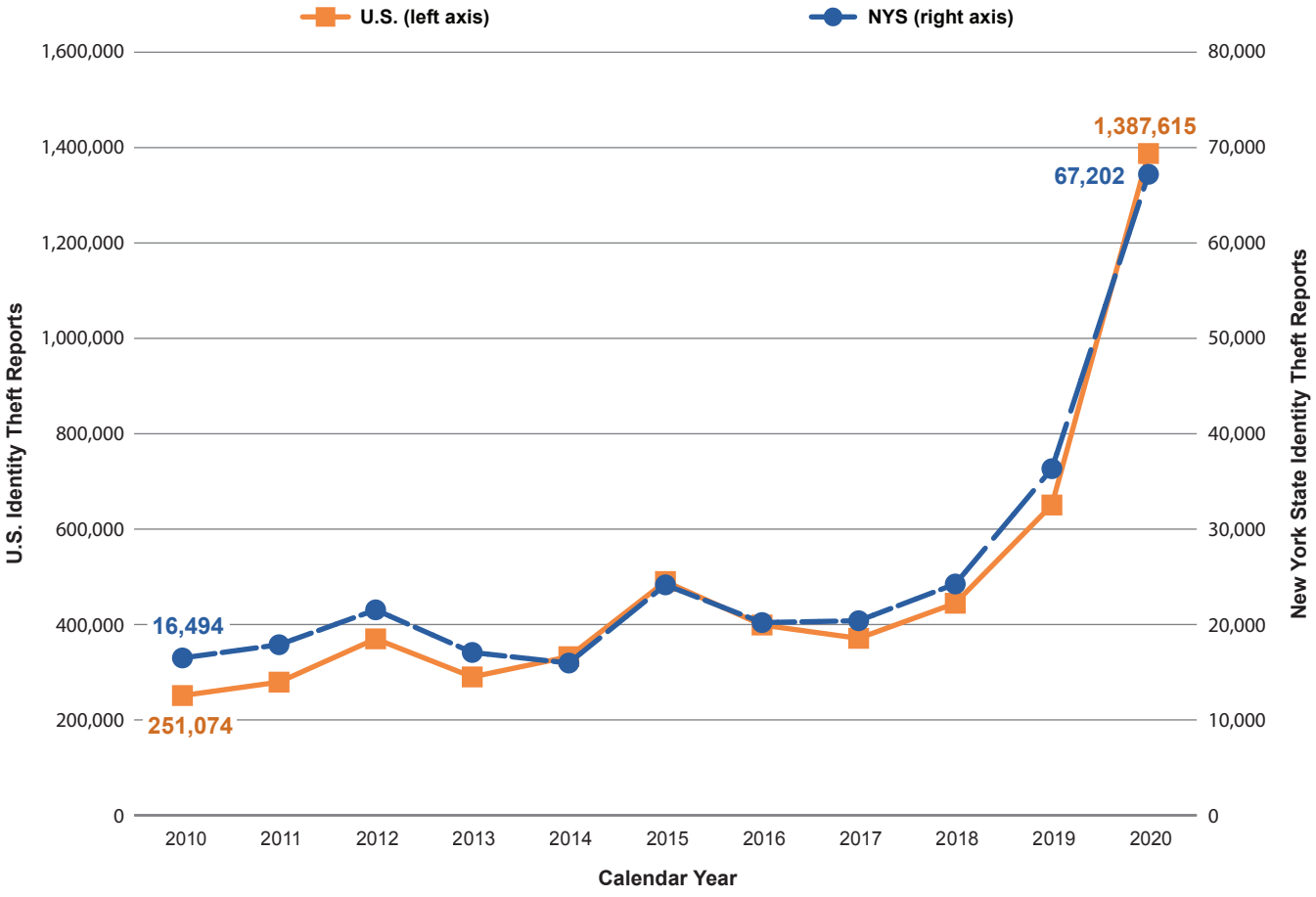
Private companies, especially credit agencies, social media providers and others that collect personal data from millions of consumers, must do more to safeguard such data. Along with their widely popular services, Facebook, Twitter and other online platforms present risks to users' private data, in part because social media providers collect large amounts of such information and encourage and facilitate sharing much of it. Among other potentially useful steps, these businesses need to make their privacy policies and settings more accessible and user friendly, and more proactively remind users of important security tips such as avoiding public posting of birthdates, email addresses, phone numbers and other personally identifiable information. Social media platforms should also urge users to regularly review privacy settings, along with information the company collects from or shares with other social media platforms.

Identity Theft Trends

Record Numbers of Identity Theft Cases Reported in 2020

New Yorkers reported a record 67,202 cases of identity theft to the Federal Trade Commission (FTC) in 2020—a jump of 85 percent from 2019 and four times the number from 2010. Nationwide reports rose sharply over the period as well, as shown in Figure 1. The FTC defines identity theft as one individual appropriating another's personally identifiable information, such as Social Security number or credit card account number, to commit fraud or theft.

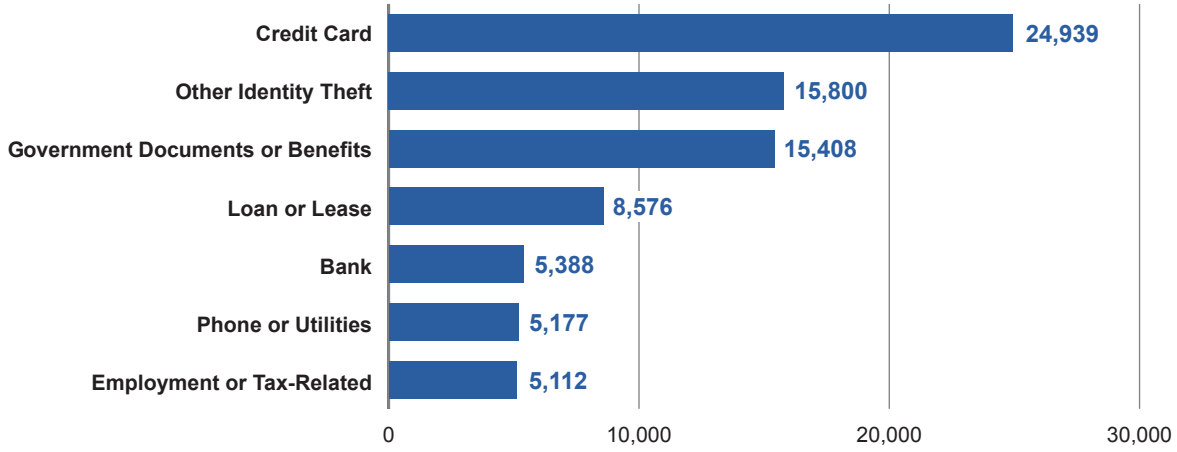
FIGURE 1
Identity Theft Reports in the U.S. and New York, 2010-2020



Source: Federal Trade Commission Consumer Sentinel Network data books 2010-2020.

Among the various types of identity theft reported by New Yorkers to the FTC, credit card fraud was the most frequently reported, representing more than a third of the total, as shown in Figure 2.[1]

FIGURE 2
Types of Identity Theft Reported by New Yorkers to the FTC, 2020
(By Total Reports)



Note: New Yorkers filed a total of 67,202 identity theft reports with the FTC in calendar year 2020. Consumers can report multiple types of identity theft for a given incident.

Source: Federal Trade Commission Consumer Sentinel Network Data Book 2020.

The incidence of credit card-related identity theft rose sharply in 2020, up by a third (6,149 cases) from the previous year. Reports involving loans or leases rose by more than 4,100, or 94 percent, while cases involving debit cards and other bank accounts or transactions were up by 50 percent.

Credit card fraud occurs when someone steals another individual's credit card information and uses it to make unauthorized purchases. Credit card fraud can occur through high-tech means, like computer hacking, or by simpler means, like stealing a wallet, obtaining the credit card information during a purchase, or accessing credit card statements thrown in the trash.

In addition to potential monetary losses, credit card fraud can severely damage a consumer's credit score if, for example, unauthorized credit card debt is incurred and then goes unpaid. The federal Fair Credit Billing Act (FCBA) provides some protection for victims of stolen credit cards. Under the FCBA, once an unauthorized credit card charge is reported, the issuer is required to follow certain investigatory procedures. During the investigation, the card holder may withhold payment on the disputed

1 Government documents or benefits fraud was the most frequent type of identity theft reported nationally in 2020, according to the FTC. The agency received over 400,000 reports last year from people who said their information was misused to apply for a government document or benefit such as unemployment insurance (UI) or others.

amount. If it is found that the charges were in fact unauthorized, the FCBA limits the holder's total liability to $50.[2]

Figure 2 also shows other types of financial identity theft, where the thief is trying to obtain credit, goods, services, or a government benefit in someone else's name. Both adults and minors can be vulnerable as victims.

Indeed, the Social Security numbers of children are regarded as highly valuable to thieves because they often do not have any information associated with them yet. In March 2019, authorities in Western New York announced that eight people had been charged with identity theft and other crimes involving the use of Social Security numbers for juveniles aged 11 to 15 who lived in other states.[3]

"Other Identity Theft" is the second largest category reported by New Yorkers and includes email or social media, insurance, medical services, online shopping or payment accounts, and investment accounts. Social media can be a ready vehicle for identity theft, given the extensive personal information many users post online. Birthdays, commonly available on Facebook and some other platforms, are often a central element of identity theft schemes. Even users who do not consciously make their birth dates available may do so inadvertently—for example, by posting a picture of a vaccine card or driver's license. Use of personal data such as mothers' maiden names that may be available through social media can create risks if those identifiers are used for online security purposes.

Threats to consumers' personally identifiable information evolve continuously, as evidenced by a warning the State Department of Financial Services (DFS) sent in March 2021 to companies that it regulates. The alert cited "an ongoing cybercrime campaign that … has already resulted in theft of sensitive data for hundreds of thousands of New Yorkers." DFS urged business executives to "take immediate action to protect consumer data." The March warning referred to a February 2021 alert regarding use of drivers' license numbers obtained from websites that offer instant online quotes for auto insurance or other products, and cited additional methods reported after the February alert.[4]

Thieves may try to steal someone's identity for reasons beyond financial gain. Other types of identity theft include medical identity theft, or using another individual's personally identifiable information to fraudulently obtain medical services, prescription drugs or medical insurance coverage; criminal identity theft, or giving false identity information to police at the time of an arrest; and identity cloning and concealment, or attempting to impersonate someone else to hide a true identity.

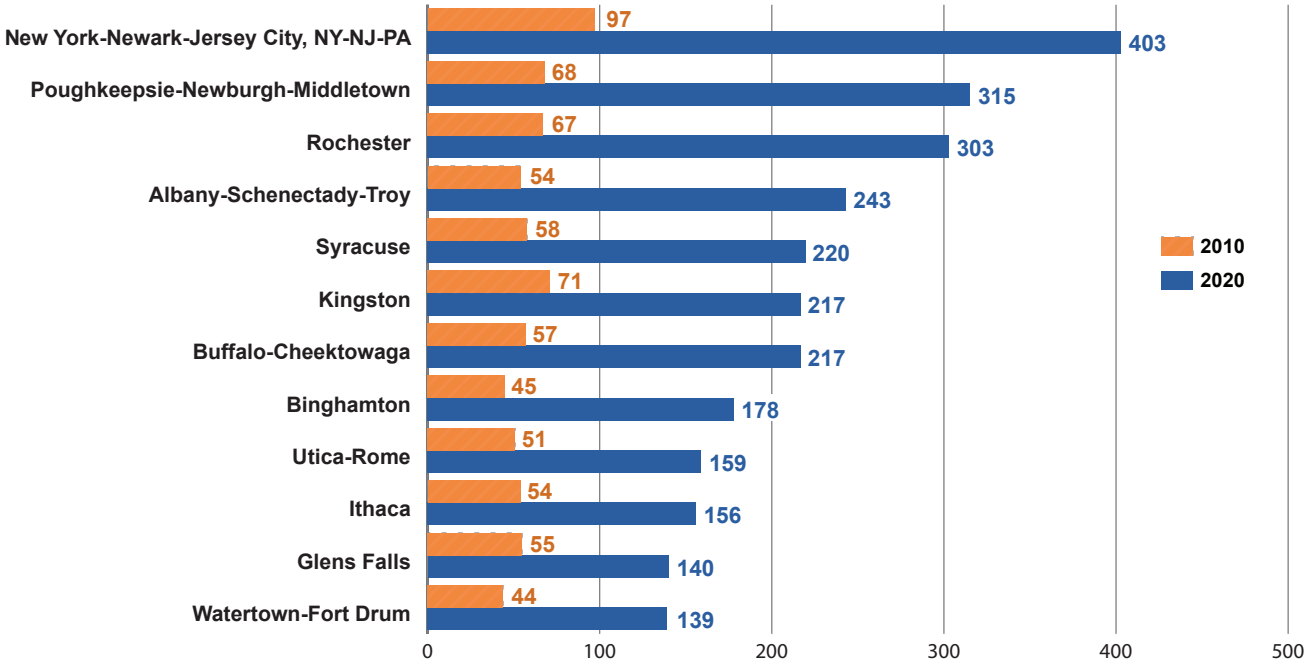
2 See Federal Trade Commission, Consumer Information, Disputing Credit Card Charges, available at https://www.consumer.ftc.gov/articles/0219-disputing-credit-card-charges.

3 "DA Flynn Announces Multiple Arrests in Identity Theft Scheme," Erie County press release, March 28, 2019, available at https://www2.erie.gov/da/index.php?q=press/da-flynn-announces-multiple-arrests-identity-theft-scheme.

4 New York State Department of Financial Services, Cybersecurity Division, Industry Letter, March 30, 2021, available at https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210330_cyber_alert_followup#_edn2.

In 2020, the New York-Newark-Jersey City metropolitan statistical area (MSA) had the highest rate of identity theft reports of any MSA that is mostly or entirely within the State, as shown in Figure 3. The Poughkeepsie-Newburgh-Middletown MSA was second.

FIGURE 3
New York Identity Theft Reports by Metropolitan Statistical Area, 2010 and 2020
(Per 100,000 population, ranked from highest to lowest based on 2020 reports)



Notes: The New York-Newark-Jersey City MSA includes New York City, Long Island and Putnam, Rockland and Westchester counties within New York State, as well as Bergen, Essex, Hudson, Hunterdon, Middlesex, Monmouth, Morris, Ocean, Passaic, Somerset, Sussex and Union counties in New Jersey, and Pike County, Pennsylvania.

Source: Federal Trade Commission Consumer Sentinel Network data for 2010 and 2020.

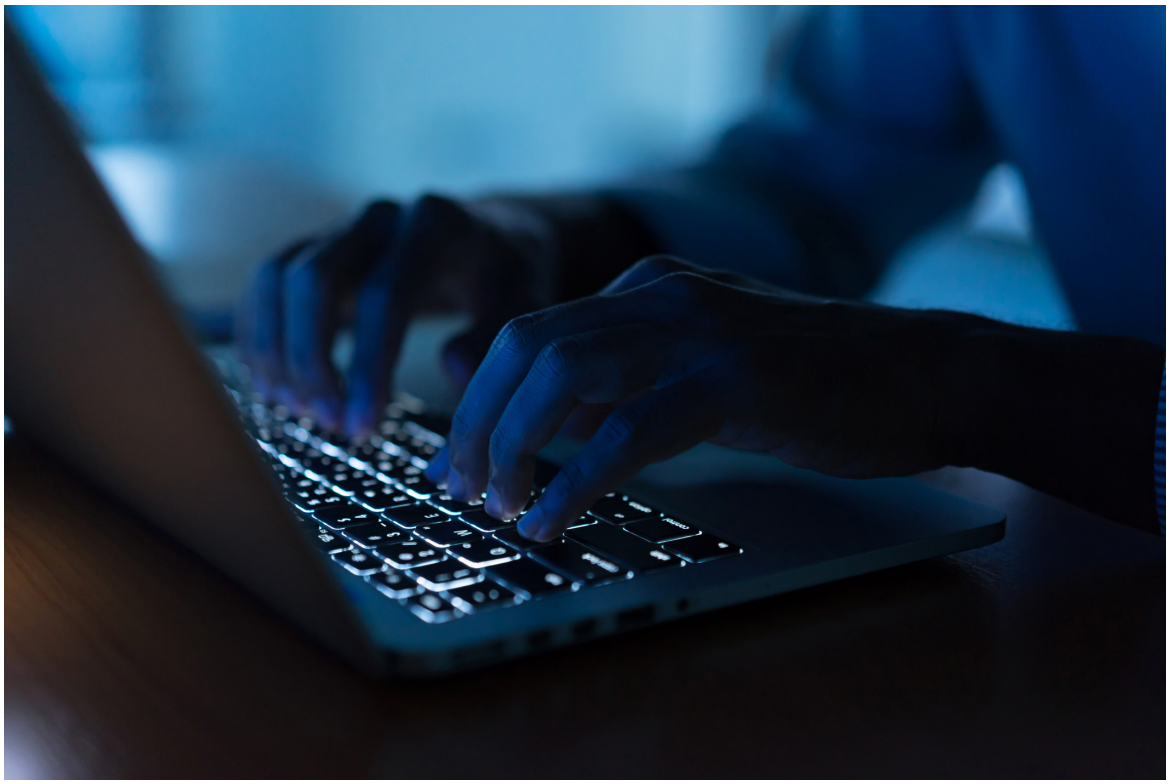
In a 2019 nationwide survey by the Pew Research Center, 28 percent of Americans said they had suffered at least one of three kinds of identity theft in the previous 12 months. The survey found that 21 percent of respondents had experienced fraudulent charges on their credit or debit cards; 8 percent had someone take over their social media or email accounts without their permission; and 6 percent had someone try to open a credit line or get a loan using their name.[5]

5 Pew Research Center, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," November 15, 2019, available at https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

Arrests and Convictions for Identity Theft Offenses in New York State

New York established the crimes of identity theft and unlawful possession of personal identification information with legislation enacted in November 2002.[6] The law defined identity theft as assuming the identity of another person to obtain goods, money, property, services or credit or to commit another crime. The unlawful possession of personal identification information relates to information such as savings, checking or credit card account numbers and the intention to use it to commit a crime.

Under the law, courts can require persons convicted of these crimes to make restitution for all costs and losses suffered by victims of identity theft or unlawful possession of personal identification information. Criminal conviction can result in up to seven years in prison for the most serious crimes. The law also allows victims to sue for damages when any person or company uses another's identity to obtain credit, goods, services or anything else of value.



6 See Chapter 619 of the Laws of 2002, available at https://nyassembly.gov/leg/?default_fld=%0D%0A&leg_video=&bn=A04939&term=2001&Summary=Y&Actions=Y&Memo=Y&Text=Y.

While identity theft complaints have surged in New York over the past decade, annual numbers of reported arrests and convictions have changed relatively little.

Most reports of identity theft do not end in arrests and convictions. Statewide, identity theft arrests averaged about 750 each year over the past decade, while courts reported an average of 450 convictions and sentencings annually, according to the State's Division of Criminal Justice Services.

The 543 arrests in State Fiscal Year (SFY) 2019-20 as reported by the State's Division of Criminal Justice Services (DCJS) were the fewest during the 10-year period shown in Figure 4. (DCJS reports arrests and convictions in each State fiscal year, April through March, while the FTC data presented earlier in this report are reported quarterly, with the latest data available through calendar 2020.) The highest reported number of arrests statewide, 887, occurred in SFY 2016-17.

Convictions and sentencings for identity theft offenses averaged 452 per year over the decade. The numbers of convictions and sentencings were significantly lower in the two most recent fiscal years compared to previous years; potential factors in these differences are not clear.

FIGURE 4
Arrests and Convictions-Sentencings for Identity Theft Offenses, SFY 2010-11 – SFY 2019-20

	2010-11	2011-12	2012-13	2013-14	2014-15	2015-16	2016-17	2017-18	2018-19	2019-20
New York State Arrests	**801**	**780**	**779**	**689**	**728**	**729**	**887**	**793**	**812**	**543**
Total Convicted-Sentenced	510	550	510	448	451	452	554	448	391	201
New York City	226	252	202	154	134	137	181	125	116	43
Rest of State	284	298	308	294	317	315	373	323	275	158

Note: Numbers of those convicted (e.g., of a felony or misdemeanor) and those sentenced (e.g., to prison, jail, probation or fined) for identity theft offenses by State fiscal year reflect separate actions. However, those arrested in one year may be convicted and sentenced in a subsequent year.

Source: Division of Criminal Justice Services Computerized Criminal History File of counts of persons age 18 or older at the time of the crime (as of 01/15/2021).

Among the State's counties, identity theft arrests and convictions are most frequent in counties with the largest populations, as shown in Figure 5. After adjusting for population, Albany County ranked first for both identity theft arrests and convictions in SFY 2019-20.

FIGURE 5
Counties with Greatest Numbers of Identity Theft Arrests and Convictions-Sentencings, SFY 2019-20

Arrests				Convictions - Sentencings			
County	Total Number	County	Per 100,000 Population	County	Total Number	County	Per 100,000 Population
New York	54	Albany	12	Nassau	29	Albany	5
Kings	50	Cortland	11	New York	21	Jefferson	3
Nassau	49	Rensselaer	9	Erie	18	Rensselaer	3
Monroe	45	Jefferson	7	Monroe	17	Monroe	2
Erie	45	Chenango	6	Westchester	17	Nassau	2
Albany	36	Monroe	6	Albany	16	Erie	2
Westchester	30	Onondaga	6	Queens	11	Westchester	2
Onondaga	27	Wayne	6	Suffolk	9	Oneida	2
Queens	25	Niagara	5	Kings	7	Saratoga	2
Bronx	21	Genesee	5	Orange	6	Dutchess	2

Sources: DCJS, Computerized Criminal History File (as of 01/15/2021) for the numbers of arrests and convictions-sentencings; and Data NY, Annual Population Estimates for New York State and Counties: Beginning 1970, available at https://data.ny.gov/Government-Finance/Annual-Population-Estimates-for-New-York-State-and/krt9-ym2k/data for the populations of counties in 2019.

The DCJS figures reflect only arrests and convictions by New York State and local authorities. Identity-related crimes can also be prosecuted under federal laws. In September 2020, for example, federal authorities announced charges against nine men for an identity theft and bank fraud scheme that allegedly affected hundreds of victims in Albany County and Onondaga County, as well as in other states. Losses to victims exceeded $1.5 million, according to the U.S. Department of Justice.[7] As detailed in the next section, fewer than one in every 10 victims of identity theft reports the incident to police.

7 U.S. Department of Justice, "Nine Indicted in Connection with Identity Theft and Bank Fraud Conspiracy," September 3, 2020, available at https://www.justice.gov/usao-ndny/pr/nine-indicted-connection-identity-theft-and-bank-fraud-conspiracy.

Costs, Characteristics and Causes of Identity Theft

Nationwide losses from all incidents of identity theft totaled $15.1 billion in 2018, according to the U.S. Justice Department.[8] The Justice Department data do not include breakdowns by state; however, New York's losses would total more than $800 million if the State's share was similar to its share of the identity theft reports to the FTC in 2018 (about 5 percent).

The Justice Department estimated that 2.8 million persons age 16 or older experienced one or more incidents of identity theft in 2018 and had out-of-pocket losses (12 percent of all identity theft victims); the remaining 88 percent had no out-of-pocket losses or losses of less than $1. Persons ages 35 to 49 and ages 50 to 64 (11 and 10 percent, respectively) had a higher prevalence of identity theft than all other age groups. In 2018, persons in the highest income category (households with annual incomes of $75,000 or more) had the highest prevalence of identity theft (12 percent). Among victims experiencing out-of-pocket losses of $1 or more, the average loss was $640 and the median loss was $100. These figures include only losses to individuals, not losses to businesses.

According to the report, more females (12 million) than males (11.2 million) experienced identity theft, but males and females had similar identity theft prevalence rates (9 percent per year). Whites (10 percent) had a higher prevalence of identity theft than Asians (8 percent), Blacks (7 percent) and Hispanics (6 percent).

The report found the most common way victims discovered identity theft was when a financial institution contacted them about suspicious activity (46 percent); 21 percent noticed fraudulent charges on their accounts. Only 7 percent of identity-theft victims reported the incident to police, but 88 percent contacted a credit card company or bank to report the incident.

Identity theft can result from as small an event as a wallet or purse being lost, or from a massive corporate data breach that exposes personal information from tens of millions of individuals. While every case of identity theft or exposure of personal data is troubling, large-scale data breaches can create serious, widespread risks for consumers. In 2017, the consumer credit reporting service Equifax announced it had experienced a data breach involving personal information of 147 million people, including an estimated 8.5 million New Yorkers.[9] In September 2018 and July 2020, respectively, the social media platforms Facebook and Twitter suffered security breaches that exposed personal data for certain users. The Twitter cyberattack targeted several cryptocurrency companies

8 See U.S. Department of Justice, Bureau of Justice Statistics, "Victims of Identity Theft, 2018," issued in April 2021, available at https://www.bjs.gov/content/pub/pdf/vit18.pdf.

9 See Official Settlement Website for the Equifax Data Breach Settlement, at https://www.equifaxbreachsettlement.com/.

regulated by the State Department of Financial Services (DFS).[10] DFS said the incident "exposed the vulnerability of a global social media platform with over 330 million total monthly active users and over 186 million daily active users, including over 36 million (20%) in the United States." Fraudulent Twitter accounts in the names of prominent individuals have been used in cryptocurrency scams that have stolen tens of millions of dollars from users of such currency, according to DFS.

In early April 2021, a hacker published online the names, birthdates, phone numbers and other personal information for more than 500 million Facebook users from 106 countries, including 32 million in the United States. While the company said the data was from 2019 and it had resolved the security failure that had allowed access to such information, its newly widespread availability online may be valuable to perpetrators of identity theft.[11] Also in April 2021, LinkedIn acknowledged that what it described as publicly available data from its members—reportedly also more than half a billion individuals—had been offered for sale online.[12]

COVID-19 Identity Theft

Along with the loss of hundreds of thousands of lives and widespread economic devastation, the COVID-19 era has been marked by new varieties of financial fraud, including new identity theft scams. Although the full impact of the pandemic on the problem of identity theft is not yet known, New Yorkers should be aware of potential scams and guard against them.[13]

The FTC has compiled identity theft complaints related to COVID-19 for 2020 through mid-March 2021, reporting 58,783 such complaints nationwide including 3,617 in New York.[14] Of the New York identity theft reports, about two-thirds or 2,375 were related to information misused to apply for a government document or benefits such as economic relief checks or unemployment insurance (UI).[15] According to the FTC, imposters are filing claims for unemployment benefits using

10 New York State Department of Financial Services, "Twitter Investigation Report," available at https://www.dfs.ny.gov/Twitter_Report.

11 Aaron Holmes, "533 Million Facebook Users' Phone Numbers and Personal Data Have Been Leaked Online," Business Insider, April 3, 2021, available at https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4.

12 See LinkedIn announcement, "An update on report of scraped data," April 8, 2021, available at https://news.linkedin.com/2021/april/an-update-from-linkedin; and Chris Stokel-Walker, "Recent Facebook, LinkedIn and Clubhouse leaks explained," Cybernews, April 15, 2021, available at https://cybernews.com/editorial/recent-facebook-linkedin-and-clubhouse-leaks-explained/.

13 See, e.g., announcements from the U.S. Department of Health and Human Services, Office of Inspector General, https://oig.hhs.gov/coronavirus/fraud-alert-covid19.asp; New York State Office of the Attorney General, https://ag.ny.gov/coronavirus#cpt; and New York State Department of Financial Services, https://www.dfs.ny.gov/consumers/coronavirus/scams.

14 See FTC Consumer Sentinel Network data for the period from January 1, 2020 to March 10, 2021, available at https://public.tableau.com/profile/federal.trade.commission#!/vizhome/COVID-19andStimulusReports/Map; data accessed March 22, 2021.

15 FTC data.

the names and personal information of people who have not filed claims. People learn about the fraud when they get a notice from their State unemployment benefits office or their employer about their supposed application for benefits.[16]

Even Erie County's top prosecutor, District Attorney John Flynn, reported receiving notice that someone used his information to file a false UI claim. "If someone tried to use my name," he said, "everybody's at risk."[17]

As of late April 2021, the State Department of Labor (DOL) said it had identified over 1.1 million fraudulent unemployment benefit claims during the COVID-19 pandemic, preventing more than $12.3 billion in stolen benefits.[18] (Multiple claims may be from the same individual.)

New Yorkers who receive tax form 1099-G for unemployment compensation that they did not apply for or collect should immediately report suspected UI fraud to DOL and suspected identity theft to the FTC and follow FTC recommendations for identity theft. These recommendations include reviewing free credit reports for signs of additional fraud from the credit bureaus and considering a credit freeze or credit fraud alert through the credit bureaus. The Internal Revenue Service (IRS) also recommends filing an identity theft complaint with 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.[19]

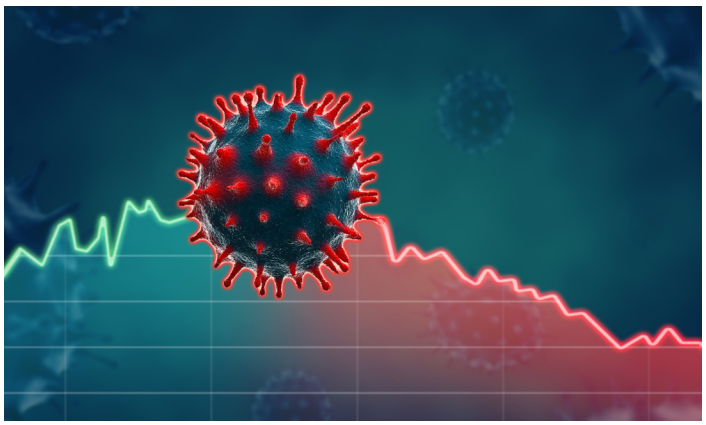
16 See FTC consumer information blog entry, "Is a scammer getting unemployment benefits in your name?" available at https://www.consumer.ftc.gov/blog/2020/06/scammer-getting-unemployment-benefits-your-name.

17 Aaron Besecker, "Unemployment Insurance scammers attempt to victimize Erie County DA," *The Buffalo News*, March 11, 2021, available at https://buffalonews.com/news/local/crime-and-courts/unemployment-insurance-scammers-attempt-to-victimize-erie-county-da/article_5ca768d0-828a-11eb-be5f-275c49da56d8.html.

18 See DOL news release, "The New York State Department of Labor Stops Fraudsters from Stealing More Than $5.5 Billion in Unemployment Benefits During Covid-19 Pandemic," available at https://dol.ny.gov/news/new-york-state-department-labor-stops-fraudsters-stealing-more-55-billion-unemployment.

19 See IRS webpage on identity theft and unemployment benefits, available at https://www.irs.gov/identity-theft-fraud-scams/identity-theft-and-unemployment-benefits.

Identity theft crimes related to COVID-19 include health care schemes in which a victim is contacted via email, social media or other means and is told that the government requires them to take a COVID-19 test or that the vaccine or a cure for the virus is available. As part of the scam, the fraudster may solicit and obtain victims' personal and health insurance information including dates of birth, Social Security numbers, financial data, Medicare and Medicaid numbers, or private health insurance information, by warning that the victim could otherwise be responsible for costs to be incurred. Such personal information can then be used to defraud government or private health care programs, among other illicit purposes.



In addition, fraudsters reportedly have attempted to leverage news of government stimulus payments by posing as someone from an official organization and asking for personal or financial information in order to facilitate federal economic relief payments. New email "phishing" attempts are also being executed, in which fraudsters may claim to be from the Centers for Disease Control and Prevention (CDC) or the World Health Organization (WHO) and attempt to use victims' fears about COVID-19 to get an individual to click on a link to install malware, steal passwords, or get access to sensitive information. Once personal or financial information is obtained, the thieves use the victims' identity to fraudulently apply for benefits under COVID-19 related programs such as the Paycheck Protection Program or for unemployment insurance. When this occurs, victims may be prevented from legitimately receiving such benefits themselves.

Fraudsters also may attempt to leverage victims' fears by asking them to pay out of pocket to get a COVID-19 vaccine or to put their name on a vaccine waiting list and, in the process, obtain Social Security, bank account or credit card information. Consumers are urged to ignore any direct call, email or advertisement that offers the vaccine in exchange for personal or financial information.[20]

20 See warnings from the Federal Trade Commission available at https://www.ftc.gov/coronavirus/scams-consumer-advice; and the Federal Bureau of Investigation (FBI) available at https://www.fbi.gov/news/pressrel/press-releases/federal-agencies-warn-of-emerging-fraud-schemes-related-to-covid-19-vaccines.

New York State's Response

Through laws, regulations and various programs, the State has taken a variety of steps to protect personal privacy and combat identity theft by improving data security practices at credit reporting agencies and other businesses, informing consumers of ways to avoid becoming victims, and assisting individuals who have suffered identity theft or whose personal information may have been compromised.

New York's Personal Privacy Protection Law, enacted in 1984, prohibits State agencies from collecting personal information unless it is "relevant and necessary" to accomplish a purpose of the agency or to implement a program specifically authorized by law. This law also protects against disclosures of personal information without consent, except in circumstances specified in the law (e.g., to the U.S. Census Bureau, pursuant to a search warrant or a court-ordered subpoena, or for inclusion in a public safety record).

In addition, the Information Security Breach and Notification Act of 2005 requires the State and any person or business owning or licensing computerized data to notify potentially affected New Yorkers of any security breach that may have resulted in the unauthorized acquisition of personal information such as Social Security, driver's license, or credit or debit card numbers.[21]

In 2008, the Consumer Protection Division of the State's Department of State (DOS) received statutory authorization to help victims of identity theft resolve problems resulting from identity theft.[22] Upon request, DOS may act as a liaison between victims and consumer credit reporting agencies to help them protect and repair their financial and credit history. Such agencies (three of the largest are TransUnion, Equifax and Experian) may be particular targets for identity theft because they collect and maintain detailed financial data on large numbers of consumers.

Regulations finalized by DOS in May 2018 require consumer credit reporting agencies operating in New York to list all proprietary products, and the fees associated with them, that are offered to consumers for preventing or mitigating identity theft, among other provisions.[23] The Division's Identity Theft Prevention and Mitigation Program is intended to inform consumers about how to protect their personal identifying information, to help them prevent identity theft and protect their identities once their information has been compromised, and to assure appropriate assistance and complaint resolution mechanisms to repair consumers' financial credit history in the event their information is compromised.[24]

21 See Chapter 442 of the Laws of 2005, available at https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A04254&term=2005&Summary=Y&Actions=Y&Floor%26nbspVotes=Y&Memo=Y&Text=Y.

22 See Chapter 279 of the Laws of 2008, available at https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A11752&term=2007&Summary=Y&Actions=Y&Memo=Y&Text=Y.

23 See the New York State Register for May 2, 2018, available at https://docs.dos.ny.gov/info/register/2018/may2/pdf/rulemaking.pdf.

24 See the New York State Department of State's description of its identity theft prevention and mitigation program, available at https://dos.ny.gov/identity-theft-prevention-and-mitigation-program.

In July 2018, the Department of Financial Services (DFS) finalized regulations requiring consumer credit reporting agencies maintaining reports on 1,000 or more New Yorkers to register with DFS and be subject to DFS "examination" as often as DFS may deem necessary. The regulations require consumer credit reporting agencies to conduct regular security risk assessments, implement and maintain policies and procedures to protect information systems, and create a written incident response plan designed to respond to and recover from any cybersecurity event materially affecting the confidentiality, integrity or availability of their information systems or the functionality of their business or operations.[25]

In 2013, recognizing that any compromise of customers' personal information held by New York State utilities "can expose many thousands of customers to identity theft and fraud," the Public Service Commission (PSC) ordered large electric, gas and water utilities to create plans to address cybersecurity issues identified by PSC staff. Those issues included, among others, additional employee training on cyber intrusion awareness, limiting access to customer data, use of next-generation security technologies, and development of procedures for response to any security breach.[26] The utilities are required to perform annual third-party audits to ensure compliance, according to the Department of Public Service. In addition, the PSC has adopted an order establishing minimum cybersecurity and privacy protections for third-party energy suppliers and companies that electronically receive and exchange utilities' customer data.[27]

State legislation enacted in 2019 requires consumer credit reporting agencies sustaining a breach of their security systems to offer affected consumers no-cost identity theft prevention services and, if applicable, identity theft mitigation services for a period up to five years.[28] Credit reporting agencies are also required to provide all information necessary for consumers to enroll in identity theft prevention and mitigation services, as well as information on how they can request a security freeze. Information subject to the law also includes data measuring an individual's unique physical characteristics, such as fingerprints, voice print and retina or iris images. All persons and businesses owning or licensing computer data that includes New Yorkers' private information must now develop, implement and maintain reasonable safeguards to ensure the security and confidentiality of the information.

25 See DFS regulations, "Cybersecurity Requirements for Financial Services Companies," available at https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default).

26 Public Service Commission, "Order Directing the Creation of an Implementation Plan," August 29, 2013, Case No. 13-M-0178.

27 Public Service Commission press release, October 17, 2019, available at https://www3.dps.ny.gov/pscweb/webfileroom.nsf/Web/3FFABD4A7F72AA5C852584960061C19F/$File/pr19093.pdf.

28 See Chapter 115 of the Laws of 2019, available at https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A02374&term=2019&Summary=Y&Actions=Y&Memo=Y&Text=Y.

The State Attorney General's Office has achieved settlements related to data breaches, including a September 2020 agreement with health insurer Anthem Inc. to resolve a 2014 incident that compromised personal information of 78.8 million U.S. customers, including 4.6 million in New York. Attackers obtained victims' names, Social Security numbers and other data. The company's 2020 settlement with various state attorneys general entailed a $39.5 million penalty and fee, including $2.7 million to New York State; Anthem had previously entered into a class-action settlement to pay for credit monitoring service for individuals whose data was breached.[29]

In response to the sharp increase in identity theft complaints during the coronavirus pandemic, law enforcement and consumer-related government agencies have taken steps to combine resources into a shared mission to combat identity theft. State agencies such as DFS, the Department of Taxation and Finance, the Office of Information Technology Services, the Department of State's Division of Consumer Protection, and the Division of Homeland Security and Emergency Services partnered to provide scam prevention tips to New Yorkers.[30] With the recent surge in stolen identities leading to unemployment fraud during the pandemic, DFS and the Department of Labor released a joint public service announcement to educate New Yorkers about identity theft.[31]

29 Office of the New York State Attorney General, "Attorney General James Helps Secure $39.5 Million After Anthem's 2014 Data Breach," press release, September 30, 2020, available at https://ag.ny.gov/press-release/2020/attorney-general-james-helps-secure-395-million-after-anthems-2014-data-breach.

30 See Department of Financial Services, et al., joint press release, January 28, 2020, available at https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202001282.

31 See DFS and DOL, joint press release, August 13, 2020, available at https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202008131.

Preventing and Mitigating Identity Theft

How to Protect Yourself Against Identity Theft

In addition to increased requirements for private businesses to responsibly safeguard personally identifiable information, as well as government agencies' consumer protection initiatives and the efforts of law enforcement, individuals can take important steps to actively protect themselves. To prevent becoming a victim of identity theft, the following simple actions are recommended:

- Limit the personal financial information in your purse or wallet, and keep Social Security cards at home.
- Carry only the credit and bank cards you need.
- Shred financial documents when they are no longer needed.
- Don't give out personal information unless you are sure you are dealing with a trusted individual, or a legitimate representative for essential governmental or business purposes.
- Use two-factor authentication for online security where possible.
- Use a password manager and/or strong passwords, including a mixture of capital letters, numbers, and symbols, and change passwords frequently.
- Check bank or credit statements regularly.
- Check credit reports regularly through AnnualCreditReport.com and other sources.
- Don't click on links sent in unsolicited email.
- Be careful using social network platforms—for example, do not make your birth date or Social Security number readily available.
- When online shopping, look for indications that the site is secure, such as a secure URL that begins with "https" (rather than "http") and a lock icon near your browser's location field.
- Use identity theft security programs on computers.
- Consider purchasing identity theft insurance or credit monitoring service and identity-theft protection.[32]

Victims should report fraud to the FTC.[33] In addition, victims can visit IdentityTheft.gov, the federal government's "one-stop" resource for people to report identity theft and create a personal recovery plan.

32 See New York State Attorney General pamphlet, "Protect Your Identity," available at https://ag.ny.gov/sites/default/files/identity_protection.pdf; and University of Wisconsin-Madison Information Technology guidance, available at https://it.wisc.edu/news/two-things-to-look-for-in-a-secure-website/.

33 See FTC ReportFraud website at https://reportfraud.ftc.gov/#/?pid=A.

New Yorkers who believe they are at risk of having their identities stolen or have become victims of identity theft can block access to their lines of credit by placing a security freeze on their credit report.[34] The State Office of the Attorney General advises consumers to request a freeze by sending a certified letter to each of the three nationwide credit reporting agencies and allowing five business days for them to freeze a credit file. Within 10 days of freezing the file, the credit reporting agencies are required to send a confirmation letter containing a password or personal identification number consumers can use to temporarily lift or permanently remove the freeze. Victims of identity theft submitting a police report or FTC identity theft affidavit cannot be charged a fee for removing or lifting a security freeze. Credit reporting agencies are allowed to charge consumers who are not identity theft victims up to $5 to remove or lift a security freeze.

Identity theft prevention services may help individuals monitor their credit accounts or restore their identities in case of identity theft. However, consumers should be aware of the limitations to such services, and it's not clear whether individuals who use them are less susceptible to identity theft, according to the U.S. Government Accountability Office.[35]

Potential Steps for Policy Makers and Businesses

While New York State has taken important steps to address the problem of identity theft, further initiatives — some broad in scope and others more targeted — have been proposed. In 2019, digital online personal privacy was specifically addressed with the introduction of the New York Privacy Act in the State Senate and Assembly.[36] The bill would impose extensive new requirements on companies that collect and process consumer data, including online social media and retail giants such as Facebook, Google and Amazon. The legislation envisions a fiduciary-like duty to protect such data and a private right of action for consumers if this duty is breached. Another wide-ranging proposal, the New York Data Accountability and Transparency Act, was proposed as part of this year's Executive Budget. The Executive's proposal called for companies to provide disclosures to consumers, limit the collection of their data, protect sensitive categories of information and create a Consumer Data Privacy Bill of Rights.[37] While these proposals have not been enacted, consideration of whether further statutory steps are necessary should continue.

34 See New York State Attorney General Webpage, "Placing a Security Freeze on Your Credit File," available at https://ag.ny.gov/sites/default/files/security_freeze.pdf.

35 See Government Accountability Office, "Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services," March 2019, available at https://www.gao.gov/assets/gao-19-230.pdf.

36 The legislation is currently introduced, as of January 2021, as A. 680 by State Assembly Member Linda Rosenthal and is available at https://assembly.state.ny.us/leg/?bn=a680; there is no Senate equivalent.

37 This proposal was introduced in January 2021 as Part II of Public Protection and General Government Article VII legislation (S. 2505 / A. 3005) and is available at https://www.budget.ny.gov/pubs/archive/fy22/ex/artvii/ppgg-bill.pdf.

Comptroller DiNapoli has proposed legislation that would require the State Office of Information Technology Services to notify other State entities within 24 hours of the discovery of any data or network security breach that may have affected other entities' data, networked services or network connection.

Among other proposals currently introduced in the State Legislature are measures that would include medical and health information within the definition of identity theft, prohibit website publishers and advertising networks from collecting personally identifying information for marketing purposes without consent, incorporate identity theft within the definition of elder abuse, and require certain businesses to offer at least two years of identity theft prevention and mitigation services in the case of a security breach. Other proposals include requiring the State Labor Department to provide at least five years of credit monitoring and identity theft surveillance services to individuals whose personal information may have been inappropriately disclosed by the Department, and requiring credit reporting agencies to furnish proof of identity theft to creditors upon a debtor's request.

Comptroller DiNapoli has been coordinating efforts with law enforcement officials from across the State to protect the public from COVID-19-related internet scams.[38] Officials from the Internal Revenue Service have been collaborating with state tax departments and private financial firms to prevent cybercriminals from using stolen information to file fraudulent tax refunds or, more recently, to fraudulently claim someone else's Economic Impact Payment. Although it does not possess any criminal jurisdiction, the FTC supports the criminal investigation and prosecution of identity theft by collecting and organizing data on identity theft reports and making this available to participating law enforcement agencies.

Governmental agencies on the federal, State and local levels should continue to seek and pursue opportunities to collaborate and combine their varied assets to combat identity theft. Working together, agencies may be able to more effectively combat the criminals who are attempting to leverage the fears and vulnerabilities of individual consumers, which have been inflamed by the pandemic.

In a report examining the 2020 Twitter cyberattack described earlier in this report, the Department of Financial Services recommended "best practices" for cryptocurrency companies. More broadly, DFS pointed to "risks posed by social media to our consumers, economy and democracy," and called for expanded cybersecurity regulation of "systemically important social media."[39]

38 See Office of the State Comptroller press release, April 29, 2020, at https://www.osc.state.ny.us/press/releases/2020/04/comptroller-dinapoli-announces-joint-effort-ulster-orange-county-district-attorneys-combat-covid-19, and press release of May 21, 2020, regarding a joint investigation with federal law enforcement officials at https://www.osc.state.ny.us/press/releases/2020/05/state-comptroller-dinapoli-statement-arrest-muge-ma-covid-related-scam.

39 "Twitter Investigation Report," ibid.

Further efforts by social media companies to avoid risks to users' privacy could play an important role in more effectively fighting identity theft. While Facebook, Instagram, Twitter and other online platforms benefit consumers in numerous ways, they also present risks to users' private data, in part because the nature of social media is to encourage public or semi-public distribution of personal information. As noted above, experts advise consumers to be careful about allowing private personal information to be available online, and specific recommendations about particular online platforms are available from various sources.[40] But social media and other online businesses may also be able to more aggressively protect the users who both benefit from their services and create profit for these companies.

One useful step beyond the responsibilities envisioned in currently proposed legislation would be for companies to more proactively remind users of important safety and security tips that are especially relevant to social media. Common examples of such best practices for users include:

- Avoid public posting of a birthdate, email address, phone number and other data that are commonly collected or even required on certain platforms.
- Limit publicly available information about locations of photographs.
- Make sure you know how to access and use the application's privacy settings.
- Regularly review your privacy settings and limit who can see your photos, activity and information to trusted friends and not the general public.
- Avoid using the Facebook Login feature to sign in to other third-party websites, as it gives those outside companies access to your information.
- If you receive a connection request from a stranger, the safest thing to do is to reject the request.
- Consider reviewing and editing your "friends" list on a regular basis. It's easy to forget who you've connected to over time, and therefore who you are sharing information with.
- Log off from social networking sites when you no longer need to be connected.[41]

40 See, for example, "Protect Your Privacy and Safety on Facebook," New York State Office of the Attorney General, available at https://ag.ny.gov/internet/protect-your-privacy-and-safety-facebook.

41 See University of Pittsburgh, Information Technology guidance, available at https://www.technology.pitt.edu/security/best-practices-safe-social-networking; and Privacy Rights Clearinghouse, Social Networking Privacy: How to be Safe, Secure and Social, available at https://privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and-social.

Consumer Protection Resources

If you believe you have been the victim of identity theft and you need help, or want to obtain more information about preventive measures against becoming a victim of identity theft, you can look to the following resources.

Consumer Credit Reporting Agencies

As described above, State law requires consumer credit reporting agencies that have sustained a breach of their security systems to offer affected consumers no-cost identity theft prevention and certain other services. Affected consumers should consider taking advantage of such services when available.

State Government Resources

Office of the New York State Comptroller: New Yorkers can report allegations of fraud involving taxpayer money across the State by calling the toll-free Fraud Hotline at 1-888-672-4555, by filing a complaint online at investigations@osc.ny.gov, or by mailing a complaint to: Office of the State Comptroller, Division of Investigations, 8th Floor, 110 State St., Albany, NY 12236.

New York State Office of the Attorney General (OAG): OAG prosecutes individuals and businesses engaged in fraudulent trade practices and provides information to consumers. For guidance on potential scams related to COVID-19, visit https://ag.ny.gov/coronavirus#cpt or the Office's Consumer Fraud Bureau's webpage at https://ag.ny.gov/consumer-frauds-bureau/identity-theft, or call the Office's General Helpline at 800-771-7755.

New York State Department of Taxation and Finance: The Department can assist if you are the victim of tax fraud—for example, where someone steals your personal information to file a fraudulent return or to claim a refund or credit. Visit https://www.tax.ny.gov/help/contact/fraud/identity-theft.htm to learn more.

New York State Department of State (DOS), Division of Consumer Protection: The Division educates and creates policies for New York's consumers, and helps to resolve consumer complaints. Visit the DOS webpage on identity theft at https://dos.ny.gov/identity-theft-prevention-and-mitigation-program.

New York State Department of Financial Services (DFS): DFS provides information, links and resources on how to recognize and avoid becoming a victim of fraud at https://www.dfs.ny.gov/consumers/scams_schemes_frauds/identity_theft. You can also file a complaint with the Department about a scam involving a financial product or service through the DFS Consumer Complaint Portal at https://www.dfs.ny.gov/complaint. For the agency's information on coronavirus-related scams, visit https://www.dfs.ny.gov/consumers/coronavirus/scams.

Federal Government Resources

Federal Trade Commission: The FTC's mission includes working to protect consumers against unfair, deceptive or fraudulent practices in the marketplace. For consumer protection information, its website is https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection.

You can also visit IdentityTheft.gov, a site hosted by the FTC that allows victims of identity theft to file complaints and will help walk you through steps for recovery.

U.S. Department of Justice (DOJ): Visit the DOJ website at https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud. The Department's National Center for Disaster Fraud website allows you to submit complaints of fraud, waste, abuse, or mismanagement related to any man-made or natural disaster, including criminal activity related to the coronavirus. You can file a complaint at https://www.justice.gov/disaster-fraud/ncdf-disaster-complaint-form.

Other components of the Department of Justice that may be helpful include:

a. Federal Bureau of Investigation, at https://www.fbi.gov/.

b. Office for Victims of Crime, which works to improve services and raise awareness for victims of crime. You can find information and resources on identity theft at https://ovc.ncjrs.gov/topic.aspx?topicid=29.

c. Task Force on Market Integrity and Consumer Fraud, established in 2018 to combat fraud against consumers—particularly the elderly, service members, and veterans—and corporate fraud that victimizes the general public. Visit the Task Force's website at https://www.justice.gov/fraudtaskforce.

Internal Revenue Service (IRS): The IRS provides links and resources on identity theft and can assist you with a tax-related fraud at https://www.irs.gov/identity-theft-central.

Federal Deposit Insurance Corporation (FDIC): The FDIC provides information for financial institutions in identity theft cases at https://www.fdic.gov/consumers/index.html.

U.S. Department of the Treasury, Office of the Comptroller of the Currency: For information on different types of consumer fraud, see https://www.occ.treas.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/types-of-consumer-fraud.html#identity.

U.S. Postal Inspection Service: For information on fraud schemes involving the mail, visit https://www.uspis.gov/tips-prevention/identity-theft.

U.S. Securities and Exchange Commission: For complaints about investment fraud and cases involving misuse of identity in connection with securities transactions, see https://www.sec.gov/.

Conclusion

Identity theft, long a significant problem in New York and across the nation, has become increasingly widespread in recent years. Ongoing growth in consumer activity and personal communications that occur online, along with increased sophistication of internet-based criminals, threaten to victimize still more New Yorkers going forward.

Individual consumers can and should take steps to guard against identity theft by protecting personal private information, consistently checking bank and credit card statements, and following other cautionary recommendations from federal and state authorities and independent experts. Social media platforms and other businesses that collect personal information from millions of individuals must take every available precaution to avoid contributing to identity theft and similar crimes involving private data. More widespread, more aggressive efforts by individuals, corporations and government may reduce risks of identity theft and reverse recent troubling increases in such crimes.

Contact

Office of the New York State Comptroller
110 State Street
Albany, New York 12236

(518) 474-4044

www.osc.state.ny.us

Prepared by the Office of Budget and Policy Analysis

Andrea Miller, Executive Deputy Comptroller
Maria Doulis, Deputy Comptroller
Pasquale Reale, Assistant Comptroller
Todd Scheuermann, Assistant Comptroller

Like us on **Facebook** at facebook.com/nyscomptroller
Follow us on **Twitter** @nyscomptroller
Follow us on **Instagram** @nys.comptroller