



March 2019

DATA BREACHES

Range of Consumer Risks Highlights Limitations of Identity Theft Services

Accessible Version

Why GAO Did This Study

Recent large-scale data breaches of public and private entities have put hundreds of millions of people at risk of identity theft or other harm. GAO was asked to review issues related to consumers' options to address risks of harm from data breaches. This report, among other things, examines information and expert views on the effectiveness of consumer options to address data breach risks. GAO analyzed available data on options, collected and analyzed related documentation, conducted a literature review of studies, and interviewed a nongeneralizable sample of 35 experts (from academia, government entities, consumer and industry organizations) and identity theft service providers to reflect a range of views.

What GAO Recommends

GAO reiterates a matter for congressional consideration and a recommendation from its 2017 report on identity theft services (GAO-17-254). In that report, GAO found that legislation requiring federal agencies that experience data breaches, including OPM, to offer certain levels of identity theft insurance coverage to affected individuals requires coverage levels that are likely unnecessary. Therefore, Congress should consider permitting agencies to determine the appropriate coverage level for such insurance. GAO also recommended the Office of Management and Budget (OMB) update its guidance for agency responses to data breaches, after analyzing the effectiveness of identity theft services relative to lower-cost alternatives. OMB did not agree or disagree and had not taken action as of early March 2019.

View [GAO-19-230](#). For more information, contact Anna Maria Ortiz at (202) 512-8678 or ortiza@gao.gov.

DATA BREACHES

Range of Consumer Risks Highlights Limitations of Identity Theft Services

What GAO Found

No one solution can address the range of potential risks from a data breach, according to interviews with academic, consumer, government, and industry experts and documentation GAO reviewed. Perpetrators of fraud can use stolen personal information—such as account numbers, passwords, or Social Security numbers—to take out loans or seek medical care under someone else's name, or make unauthorized purchases on credit cards, among other crimes. Foreign state-based actors can use personal information to support espionage or other nefarious uses.

Public and private entities that experience a breach sometimes provide complimentary commercial identity theft services to affected individuals to help monitor their credit accounts or restore their identities in cases of identity theft, among other features. Consumers also may purchase the services. As of November 30, 2018, the Office of Personnel Management (OPM) had obligated about \$421 million for a suite of credit and identity monitoring, insurance, and identity restoration services to offer to the approximately 22 million individuals affected by its 2015 data breaches. As of September 30, 2018, about 3 million had used the services and approximately 61 individuals had received payouts from insurance claims, for an average of \$1,800 per claim. OPM re-competed and awarded a contract to the previously contracted company in December 2018.

GAO's review did not identify any studies that analyzed whether consumers who sign up for or purchase identity theft services were less subject to identity theft or detected financial or other fraud more or less quickly than those who monitored their own accounts for free. A few experts said consumers could sign up for such services if offered for free. Credit monitoring may be convenient for consumers and personalized restoration services may help identity theft victims recover their identities, but such services do not prevent fraud from happening in the first place. The services also do not prevent or directly address risks of nonfinancial harm such as medical identity theft.

Consumer, government, and industry experts highlighted other free options, including a credit freeze, which prevents one type of fraud. A freeze restricts businesses from accessing a person's credit report—and can prevent the illicit opening of a new account or loan in the person's name. A provision of federal law that took effect in September 2018 made it free for consumers to place or lift credit freezes quickly at the three nationwide consumer reporting agencies (Equifax, Experian, and TransUnion). Consumers also can regularly monitor their accounts and review their credit reports for free every 12 months. In addition, they can take advantage of free federal assistance such as the guidance on the Federal Trade Commission's IdentityTheft.gov website.

Finally, large amounts of personal information are outside of consumers' control and bad actors can use stolen information for years after a breach. Therefore, experts noted that data security at entities that hold such information—and efforts to make stolen information less useful for identity thieves, through use of new identity verification technologies, for example—are important ways to mitigate risks of harm for consumers.

Contents

Letter		1
	Background	4
	Limited Information Is Available on Effectiveness of Options after Data Breaches, but Credit Freezes Can Prevent New-Account Fraud	10
	Federal Agencies Provide Assistance to Consumers Affected by Data Breaches and Identity Theft	22
	Agency Comments	34
<hr/>		
Appendix I: Objectives, Scope, and Methodology		35
Appendix II: What Can Consumers Do After a Data Breach?		39
Appendix III: GAO Contacts and Staff Acknowledgements		45
Appendix IV: Accessible Data		46
	Data Table	46
<hr/>		
Figures		
	Figure 1: Overview of Credit Freezes	18
	Figure 2: Enrollment in Identity Theft Services Offered by Office of Personnel Management, October 2015–September 2018	28
	Figure 3: What Can Consumers Do After a Data Breach?	40
	Accessible Data for Figure 2: Enrollment in Identity Theft Services Offered by Office of Personnel Management, October 2015–September 2018	46

Abbreviations

CFPB	Consumer Financial Protection Bureau
FTC	Federal Trade Commission
IRS	Internal Revenue Service
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIN	personal identification number

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



March 27, 2019

The Honorable Frank Pallone
Chairman
Committee on Energy and Commerce
House of Representatives

The Honorable Jan Schakowsky
Chair
Subcommittee on Consumer Protection and Commerce
Committee on Energy and Commerce
House of Representatives

The Honorable Diana DeGette
Chair
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
House of Representatives

Sensitive personal information—such as Social Security numbers or dates of birth—can be exposed in several ways, including on a very large scale through a data breach.¹ For example, major retail and hotel chains have suffered data breaches that exposed the identifying information, including financial account or Social Security numbers, of millions of people. Consumers whose information is exposed can be at risk of a range of harms, including identity theft or fraud. Consumers can try to prevent or mitigate these harms in a number of ways, such as monitoring their credit reports and credit card statements for suspicious activity, or placing a credit freeze that restricts access to their credit report. They also may enroll in free or fee-based identity theft services.² Private-sector

¹A data breach generally refers to an unauthorized or unintentional exposure, disclosure, or loss of an organization’s sensitive information. This information can include personally identifiable information, such as Social Security numbers, or financial information, such as credit card numbers. A data breach can be inadvertent, such as from the loss of an electronic device, or deliberate, such as from the theft of a device or a cyber-based attack by a malicious individual or group, agency insiders, foreign nations, or terrorists.

²We use “identity theft services” to refer to commercial products that generally provide tools intended to help consumers detect identity theft and restore their identity if it has been compromised.

and government entities that experienced data breaches have provided these services to millions of affected consumers.

In March 2017, we reported on the potential benefits and limitations of commercially available identity theft services and factors that affect public- and private-sector decision-making about them.³ Since that time, additional large-scale data breaches have occurred and Congress passed legislation that enhances some of the options available to consumers to prevent or mitigate identity theft. You asked us to review issues related to actions consumers can take to address risks of harm from data breaches. This report examines (1) information and expert views on the effectiveness of options consumers can use to prevent or address the risks resulting from data breaches; and (2) federal assistance available to help consumers understand these options, including the status of one matter for congressional consideration and one recommendation relating to these issues in our 2017 report.

To address the first objective, we conducted a literature review to identify any studies or independent research on the effectiveness of consumers' options for mitigating or preventing harm from exposure of personal information. We also searched for studies that examined consumer attitudes and behavior following data breaches, and harms to individuals from data breaches. We interviewed a nongeneralizable sample of experts and private companies that provide identity theft services to consumers.⁴ Specifically, we interviewed representatives of 35 entities in the following categories: academic or independent research institution (4); consumer or privacy research and advocacy (10); industry association or identity theft service provider, or industry consultant (12); and federal or state government (9). We selected the experts and identity theft service providers to represent a range of perspectives. We also reviewed provisions in the Economic Growth, Regulatory Relief, and Consumer Protection Act, enacted in May 2018, that address credit freezes and

³GAO, *Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud*, [GAO-17-254](#) (Washington, D.C.: Mar. 30, 2017).

⁴Throughout this report, we use certain qualifiers when describing responses from interview participants, such as "few," "some," and "most." While we define few as a small number such as two or three, the specific quantification of other categories depends on the overall numbers of interviewees who addressed a specific topic, and is discussed in more detail in appendix I. We defined experts as those with academic research backgrounds or professional expertise gained from employment in consumer and industry policy organizations, as well as federal and state government staff with specific positions of responsibility in consumer protection.

fraud alerts (two tools for preventing one type of identity theft).⁵ Furthermore, we reviewed the evidence collected for the 2017 GAO report on identity theft services.⁶

To address the second objective, we reviewed documentation and interviewed staff from the Federal Trade Commission (FTC), Consumer Financial Protection Bureau (CFPB), and Office of Personnel Management (OPM). We analyzed data from the company that contracted to provide identity theft services to individuals affected by two data breaches at OPM in 2015. We assessed the reliability of the data by interviewing agency officials and reviewing documentation about the systems used to store the data. We found the data to be reliable for purposes of this reporting objective. We also reviewed documentation and interviewed agency staff about the development, implementation, and assessment of their consumer education materials and other resources and assistance. We compared these activities against a 2014 Executive Order on the security of consumer financial transactions, key practices for consumer education planning identified in our prior work, and federal standards for internal control.⁷ In addition, we followed up on recommendations made in our 2017 report. For more information on our scope and methodology, including the organization representatives we interviewed, see appendix I.

We conducted this performance audit from November 2017 to March 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

⁵Pub. L. No. 115-174, § 301(a), 132 Stat. 1296, 1326 (2018) (codified at 15 U.S.C. § 1681c-1(i)).

⁶[GAO-17-254](#).

⁷Exec. Order No. 13681, 79 Fed. Reg. 63491 (Oct. 23, 2014). See GAO, *Digital Television Transition: Increased Federal Planning and Risk Management Could Further Facilitate the DTV Transition*, [GAO-08-43](#) (Washington, D.C.: Nov. 19, 2007); and *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014). Also see Office of Management and Budget, *Preparing for and Responding to a Breach of Personally Identifiable Information*, M-17-12 (Washington, D.C.: Jan. 3, 2017).

Background

Harm from Exposure of Personal Information

Individuals' sensitive personal information can be lost, stolen, or given away.⁸ Once exposed, individuals' information can be misused to commit identity theft, fraud, or inflict other types of harm. Identity theft occurs when individuals' information is used without authorization in an attempt to commit fraud or other crimes. In 2016, according to the Bureau of Justice Statistics, an estimated 26 million people—10 percent of U.S. residents aged 16 or older—reported that they had been victims of identity theft in the previous year.⁹ One potential source of identity theft is a data breach at an organization that maintains large amounts of sensitive personal information. Recent data breaches include the 2018 breach of Marriott International's Starwood guest registration database, which may have exposed information of millions of individuals, and the 2017 data breach at Equifax, Inc., a nationwide consumer reporting agency, which exposed identifying information of at least 145.5 million people.¹⁰ The types of harm that can result from exposure of sensitive personal information include the following:

⁸Identity thieves can obtain sensitive personal information through various methods. For instance, thieves can use phishing to trick individuals or employees of an organization into sharing their own or others' sensitive personal information. Phishing uses authentic-looking, but fake, emails to request information from users or direct them to a fake website that requests information. Identity theft also can occur as a result of the loss or theft of data (a lost or stolen wallet or a thief digging through household trash). Some individuals may reveal sensitive information willingly, such as on social media accounts, which when combined with other information can allow fraudsters to steal identities.

⁹Department of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2016* (Washington, D.C.: January 2019).

¹⁰We use "nationwide consumer reporting agency" to refer to the Fair Credit Reporting Act's term "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis." The act defines such an agency as one that regularly engages in the practice of assembling or evaluating, and maintaining public record information and credit account information regarding consumers residing nationwide for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity. 15 U.S.C. § 1681a(p). The three agencies that operate nationwide (Equifax, Experian, and TransUnion) provide reports commonly used to determine an individual's eligibility for credit, employment, and insurance.

- **Financial fraud from identity theft**, which can include
 - **new-account fraud**, in which thieves use identifying data, such as Social Security and driver's license numbers, to open new financial accounts without that person's knowledge; and,
 - **existing-account fraud**, which is more common and entails the use or takeover of existing accounts, such as credit or debit card accounts, to make unauthorized charges or withdraw money.¹¹
- **Tax refund fraud**, which occurs when a Social Security number or other personally identifiable information is used to file a fraudulent tax return seeking a refund.¹²
- **Government benefits fraud**, which occurs when thieves use stolen personal information to fraudulently obtain government benefits. For example, the Social Security Administration has reported that personal information of beneficiaries has been used to fraudulently redirect the beneficiary's direct deposit benefits.¹³
- **Medical identity theft**, which occurs when someone uses an individual's name or personal identifying information to obtain medical services or prescription drugs fraudulently, including submitting fraudulent insurance claims.
- **Synthetic identity theft**, which involves the creation of a fictitious identity, typically by using a combination of real data and fabricated

¹¹According to the Bureau of Justice Statistics, for 85 percent of identity-theft victims in 2016, the most recent incident involved misuse or attempted misuse of only one type of existing account, such as a credit card or bank account. Approximately 1 percent of those 16 or older experienced the opening of a new account or other misuse of personal information apart from misuse of an existing account. See Bureau of Justice Statistics, *Victims of Identity Theft, 2016*. While existing-account fraud is a significant problem, existing laws limit consumer liability for such fraud. As a matter of policy, some credit and debit card issuers may voluntarily cover all fraudulent charges. For example, for unauthorized credit card charges, cardholder liability is limited to a maximum of \$50 per card. 15 U.S.C. § 1643; 12 C.F.R. § 1026.12. For unauthorized automated teller machine or debit card transactions, the Electronic Fund Transfer Act generally limits consumer liability, depending on how quickly the consumer reports the loss or theft of the card. See 15 U.S.C. § 1693g; 12 C.F.R. §1005.6.

¹²GAO, *Identity Theft: IRS Needs to Strengthen Taxpayer Authentication Efforts*, [GAO-18-418](#) (Washington, D.C.: June 22, 2018).

¹³For a related GAO report, see *Social Security Numbers: OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display*, [GAO-17-553](#) (Washington, D.C.: July 25, 2017).

information. The federal government has identified synthetic identity theft as an emerging trend.¹⁴

- **Child identity theft**, which occurs when a child's Social Security number or other identifying information is stolen and used to commit fraudulent activity.
- **Other types of fraud** that occur when personal information is used; for example, to set up mobile phone or utility accounts, or to engage in activities such as applying for employment or renting a home.

The harms caused by exposure of personal information or identity theft can extend beyond tangible financial loss, including the following:

- **Lost time.** Victims of identity theft or fraud may spend significant amounts of time working to restore their identities. In 2016, according to the Bureau of Justice Statistics survey of identity victims, most victims resolved issues in 1 day or less but about 1 percent of victims spent 6 months or more resolving their identity theft issues.¹⁵
- **Emotional distress and reputational harm.** Exposed information also can cause emotional distress, a loss of privacy, or reputational injury. In 2016, according to the Bureau of Justice Statistics, about 10 percent of those who experienced identity theft reported suffering severe emotional distress.
- **Harm from state-based actors.** State-sponsored espionage can cause harm to individuals when nations use cyber tools as part of information-gathering, espionage, or other nefarious activities.

¹⁴GAO, *Highlights of a Forum: Combating Synthetic Identity Fraud*, [GAO-17-708SP](#) (Washington, D.C.: July 26, 2017). For example, individuals may face difficulties obtaining credit if their Social Security number has been used as part of a synthetic identity to commit fraud, or may face health risks if their records are connected to someone else. Synthetic identity fraud has grown significantly in recent years and resulted in significant financial losses to the financial industry and federal government.

¹⁵Department of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2016* (January 2019).

Consumers' Options to Address Risks or Harm

Options available to consumers to help prevent or mitigate identity theft include actions they can take on their own (generally for free) or services they can purchase.¹⁶

Actions individual consumers can take themselves include the following:

- **Placing a credit freeze.** A credit or security freeze restricts potential creditors from accessing a credit report until the consumer asks the agency to remove or temporarily lift the freeze.
- **Placing a fraud alert.** A fraud alert on a credit report requires businesses to verify a consumer's identity before they issue credit.
- **Monitoring accounts and other information.**¹⁷
 - **Reviewing free annual credit reports.** Individuals can request one copy of their credit report every 12 months (available for free at AnnualCreditReport.com) from each of the three nationwide consumer reporting agencies.¹⁸
 - **Reviewing financial statements and other accounts.** Individuals can review bank and other financial statements regularly for suspicious activity and make use of automatic transaction alerts and other free features that financial institutions offer to detect potential fraud. Individuals also can regularly review mobile phone or utility accounts for unusual activity.
 - **Reviewing health insurance benefits explanations and medical information.** Individuals can review explanation-of-benefits statements from their health insurer to detect fraudulent insurance claims or monitor their files at their healthcare providers to detect unauthorized use of medical services.

¹⁶See [GAO-17-254](#) for additional details on these options.

¹⁷Department of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2016* (January 2019). The survey found that the most common ways victims discovered identity theft was by being contacted by a financial institution (about 48 percent) or noticing fraudulent charges on an account (about 19 percent). About 1.4 percent of victims said they discovered the theft through a credit report or credit monitoring service.

¹⁸Individuals can use other mechanisms to request and review credit reports from other consumer reporting agencies every year for free.

Consumers also can obtain various free or fee-based **identity theft services**, which are commercial products that generally offer tools intended to help consumers detect identity theft and restore their identity if it has been compromised. The private research firm IBISWorld estimated that the U.S. market for identity theft services was about \$3 billion annually in 2015–2017.¹⁹ The services may be marketed directly to individuals for a monthly or annual fee. In addition, private- and public-sector entities that have experienced data breaches sometimes purchase these services and offer them to affected individuals at no cost.²⁰

- Identity theft services most often include
 - **credit monitoring**, which tracks an individual’s credit reports and sends alerts about potentially suspicious activity;
 - **identity monitoring**, which aims to monitor other sources such as public records and illicit websites (sometimes referred to as the “dark web”);
 - **identity restoration**, which provides a range of services to recover from identity theft; and
 - **identity theft insurance**, which reimburses individuals for certain costs related to the process of restoring identities.

Other actions consumers can take to protect their identity include adoption of certain data security practices and early filing of tax returns. Data security practices can help protect sensitive information. For example, individuals can change or avoid sharing or re-using passwords, and make use of strong passwords and authentication options on online accounts; properly safeguard or shred sensitive paper documents; and limit access to their sensitive information on social media. Filing a tax return early reduces the risk of tax refund fraud, and some victims of tax refund fraud may be eligible for an Identity Protection Personal Identification Number (PIN)—issued by the Internal Revenue Service (IRS)—to prevent future fraud. To protect their Social Security benefits,

¹⁹See IBISWorld, *Identity Theft Protection Services in the US*: Industry Market Research Report. We cited the reports published in April 2015 and April 2016 in [GAO-17-254](#); and accessed the August 2017 report at <https://www.ibisworld.com/industry-trends/specialized-market-research-reports/technology/computer-services/identity-theft-protection-services.html>, on August 30, 2018.

²⁰For example, in response to breaches of its databases in 2015, OPM offered identity theft services to approximately 22 million people affected by the breaches.

individuals can set up an online account at the Social Security Administration to monitor their benefits accounts.

Limited Information Is Available on Effectiveness of Options after Data Breaches, but Credit Freezes Can Prevent New-Account Fraud

We did not identify any studies that analyzed whether consumers who sign up for or purchase identity theft services encounter fewer instances of identity theft or detect instances of financial or other fraud more—or less—rapidly than consumers who take steps on their own. Views of experts varied, but most said identity theft services have limitations and would not address all data breach risks. Most experts also said that a credit freeze, which consumers place on their own for free, is a useful way to prevent one type of financial fraud—the illegal opening of new credit accounts in consumers’ names. Based on our review and discussions with experts, consumers can consider four factors when deciding on options to address risks after a data breach: the extent to which an option might prevent fraud; the cost of an option; its convenience; and the type of information that was exposed and may be at risk.

No Independent Research Assesses Effectiveness of Consumer Options to Address Risks after Data Breaches

Information that can help consumers assess their options for mitigating and addressing the risks of identity theft and other harm from data breaches is limited. Specifically, we did not identify any studies that analyzed whether consumers who sign up for free or purchase identity theft services encounter fewer instances of identity theft or detect instances of financial or other fraud more—or less—rapidly than consumers who take steps on their own for free—such as monitoring their credit reports or placing a credit freeze. For consumers who experienced identity theft, we did not find any studies that compared the effectiveness of free options to help consumers recover from identity theft with commercial identity restoration services. In addition to searching databases of scholarly publications and other sources, a range of academic, consumer, government, and industry experts we interviewed

told us that they were unaware of any specific independent studies on the effectiveness of consumer options.²¹

We interviewed representatives of seven companies that provide identity theft services about how they assess the effectiveness of their services and found that what they measure does not directly address how effective these services would be in mitigating the risks of identity theft compared with options consumers can take on their own. For example, two company representatives said that their services focus on detection of fraudulent activity or assistance after identity theft has occurred, rather than on prevention of identity theft or other harms. The representatives of each of the providers said that their companies generally measure how customers use their products and services; customer satisfaction (for example, through surveys or other feedback); and whether the products work as intended (for example, whether alerts of fraudulent activity are successfully delivered to customers or customers can successfully access the company's website when they need to). Companies that offer identity restoration services also measure the rate at which they complete the process of recovering stolen identities. While it is not possible to prevent identity fraud, four representatives said that early detection of fraud is important as it allows consumers to address potential fraud more quickly.

FTC, a primary source for assistance to consumers on issues related to data breaches and identity theft, has advised consumers that the effectiveness of services that offer identity monitoring depends on factors such as the kinds of databases the service provider monitors, how well the databases collect information, and how often the service provider

²¹See Vyacheslav Mikhed and Michael Vogan, *How Data Breaches Affect Consumer Credit* (Philadelphia, Penn.: November 2017). The study used the 2012 South Carolina Department of Revenue data breach as a natural experiment to study how data breaches and news coverage about them affect consumers' interactions with the credit market and their use of credit. The study found that some consumers directly exposed to the breach protected themselves against potential losses from future fraudulent use of stolen information by monitoring their files and freezing access to their credit reports. The response of consumers only exposed to news about the breach was negligible. As part of their analysis, the researchers measured the extent to which affected individuals signed up for credit monitoring services, credit freezes, fraud alerts, or opted out of receiving pre-screened offers of credit. The study found that the most frequent options chosen were credit monitoring services and credit freezes. The researchers also found that more individuals opted to place freezes on their credit reports than the researchers had predicted.

checks each database.²² For example, FTC suggests that consumers ask if service providers check databases that show payday loan applications or changes in addresses for misuse of their information as part of identity monitoring. In reviewing consumer education and promotional materials on the websites of five identity theft service companies we contacted that offer identity monitoring, we found that three providers included information about which types of databases they monitor; the other two did not.²³

Government and commercial entities—such as federal agencies and retail stores—that decide to purchase identity theft services to offer to affected individuals after a breach of their data do not necessarily base their decision on how effective these services are. Rather, according to industry and some government representatives we interviewed, some base their decisions on federal or state legal requirements to offer such services and the expectations of affected customers or employees for some action on the breached entities' part. Representatives of retail and banking associations we interviewed indicated that it has become the industry standard to offer 1 year of credit or identity monitoring services in the wake of a data breach. One industry representative said that in some cases the decision is not based on the effectiveness of the services.²⁴ States such as California require companies to offer some type of identity theft service after a data breach.²⁵ Moreover, Connecticut requires health insurers and certain health care-related companies to offer identity theft services following an actual or suspected data breach. In 2017, we reported that companies do not assess the effectiveness of an identity theft provider's services when selecting a vendor to provide such services. Rather, they consider other selection factors, including price,

²²Federal Trade Commission, *Consumer Information: Identity Theft Protection Services*, <https://www.consumer.ftc.gov/articles/0235-identity-theft-protection-services>; accessed on July 10, 2018.

²³We reported in 2017 that the Consumer Federation of America offers guidance to individuals and entities on selecting identity theft service providers: Consumer Federation of America, *Best Practices for Identity Theft Services, Version 2.0* (Washington, D.C.: Nov. 17, 2015).

²⁴Once exposed, there is no time limit on the potential for identity thieves to use such information to commit fraud.

²⁵Massachusetts enacted a law in 2019 that requires companies that experience a breach in which Social Security numbers are disclosed, or reasonably believed to have been disclosed, to offer credit monitoring services at no cost for at least 18 months, or 42 months if the company is a consumer reporting agency, among other things.

reputation, capacity to respond quickly to large-scale breaches, and ability to provide comprehensive post-breach services, such as complying with statutory notification requirements. But companies that purchase identity theft services may be in a position to obtain more detailed information from potential providers than is publicly available to consumers.²⁶

Views of Experts Varied, but Most Said Identity Theft Services Have Limitations and Would Not Address All Data Breach Risks

In the absence of independent evidence of the effectiveness of identity theft mitigation options, we interviewed representatives and reviewed consumer education materials, working papers, and articles from academic, consumer, industry, and government entities. No one solution can protect against the full range of risks to individuals whose personal information was exposed in a data breach, based on our review of documentation and the views of academic, consumer, government, and industry experts. We obtained perspectives on the value of options available to consumers. The following summarizes key observations:

Identity theft services. Representatives of 9 of the 10 consumer groups we interviewed generally viewed credit or identity monitoring (or both) to be of limited value. However, one consumer group representative noted that identity monitoring might be useful in circumstances in which Social Security numbers were compromised. In addition, a few consumer group representatives indicated that consumers could consider signing up for such services if they are offered for free. If identity theft services are not free, FTC and CFPB consumer education materials recommend that consumers consider the benefits and limitations of such services and compare them to free or low-cost options before signing up. A few

²⁶For example, providers can share the types, number, and frequency of databases the services monitor or the number of restoration cases they successfully complete. The Consumer Federation of America published guidance on the factors breached entities should consider in selecting identity theft service providers. For example, the organization recommends that companies whose breaches exposed Social Security numbers may want to request information about services that monitor public records, proprietary commercial databases, change of address records, and other databases. In our 2017 report, we indicated that federal and private-sector entities that purchased identity theft services in response to a data breach said they received information from the providers about the take-up rate (percentage of people offered free services who enrolled), and that they monitor how quickly and effectively the providers responded to inquiries or concerns.

consumer groups and one academic highlighted that consumers may not fully understand the limitations of signing up for identity theft services. A few consumer group representatives and one industry and state government representative cautioned that free services may be offered for only 1 or 2 years; exposed information can be used for identity theft or other harms over a much longer period. For example, in 2017, we reported that nation-state actors that steal consumer data as part of their espionage activities can wait much longer than a private identity thief to use compromised information (if at all), according to one identity theft service provider. In addition, CFPB consumer information and a few consumer group representatives noted that consumers should be aware that some services may try to charge consumers after the free period ends.

Some consumer group and one industry representatives also said that the value of one feature of identity monitoring—dark web monitoring—is unclear. One representative said that there is nothing new that consumers can do once they learn their information was found on an illicit website. Rather, they must continue to monitor their accounts as they already should have been doing. In addition, one consumer group representative indicated that these services may provide consumers with a false sense of security.

Experts we interviewed for our 2017 report said that identity restoration in particular could be helpful to consumers. FTC staff and one consumer group representative we interviewed said that one-on-one assistance can be helpful. Identity restoration typically is included with other identity theft services rather than offered as a stand-alone service. However, the level of service provided in identity restoration can vary substantially—some providers offer individualized hands-on assistance, while others largely provide self-help information that is of more limited value. In our 2017 report, we also found that another feature of identity theft services, identity theft insurance, may provide minimal benefits for consumers. More details about identity theft insurance appear later in this report.

Options to prevent fraud or harm unrelated to credit accounts.

Consumers have limited options to mitigate risks of other harms from data breaches, such as medical identity theft and identity theft tax refund fraud. Commercial identity theft services, credit freezes, and fraud alerts do not directly address these risks. Some consumer, government, and industry representatives cited self-monitoring as a way for consumers to be on the alert for these other types of fraud.

Consistent with our 2017 report, identity theft service providers we interviewed generally indicated that their products and services do not directly monitor for these types of fraud. However, two noted that they would assist with any identity restoration involving medical identity theft, tax refund fraud, or government benefits fraud (such as fraudulently redirecting Social Security benefits). Identity theft services also may address these types of fraud indirectly—for example, detecting a fraudulent change of address can prevent sensitive health insurance information from being redirected to the fraudster. A few consumer groups said that consumers may not understand which risks commercial identity theft services address. Additionally, we reported in 2017 that identity theft services do not address non-financial harms, such as emotional distress, embarrassment, and harm to one’s reputation. For example, a House Committee report on the OPM data breaches noted that the information stolen from background investigations included some of the most intimate and potentially embarrassing aspects of a person’s life, such as mental health history, misuse of alcohol or drugs, or problems with gambling.²⁷ Identity theft services also may be of limited value in cases of nation-state espionage. For example, in 2017, we reported that when the source of the data breach appears to be a nation state (as opposed to a private party), the risk of the information being sold for monetary purposes is likely to be lower, according to an FTC representative.

Importance of data security. In the view of some experts, entities such as the federal government and private companies that hold consumer data have a responsibility to protect those data.²⁸ A few experts said that the burden should not be on consumers to protect data they do not control. Except in certain circumstances, companies are generally not required to be transparent about the consumer data they hold or how they

²⁷ *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, House Committee on Oversight and Government Reform, 114th Congress (Sept. 7, 2016).

²⁸ We previously reported on data security and data protection at entities that store sensitive personal information. See GAO, *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*, [GAO-18-559](#) (Washington, D.C.: Aug. 30, 2018); and *Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer Reporting Agencies*, [GAO-19-196](#) (Washington, D.C.; Feb. 21, 2019).

collect, maintain, use, and secure these data.²⁹ Identity theft service providers may contract with third parties such as consumer reporting agencies or with third-party identity monitoring providers, such as dark web monitoring services. Moreover, one consumer group representative noted that identity monitoring services require consumers to provide additional personal information to enroll—which also could be compromised if the service provider’s information were breached.

Finally, consumer group and government researchers we interviewed suggested other options that entities can (or already) use to address risks of harm. For example, one government researcher noted that financial institutions have started to use multifactor authentication and other technologies that can help institutions verify a consumer’s identity and thus help prevent fraud. Multifactor authentication involves first logging into an online account using the traditional username and password, and then the institution sending a verification code to a mobile phone or e-mail address that the consumer must enter as part of the log-in process. In addition, one researcher noted that some institutions have started to use facial recognition technology, or to ask an account holder to provide answers to questions such as the size of the account holder’s last deposit.³⁰ Other biometric technologies such as fingerprint recognition on mobile phones, or one-time passcodes that are synced with financial institutions’ websites, also can help, according to one researcher and one consumer group representative. Other strategies can focus on reducing the riskiness of breaches by making information less useful for purposes of committing identity theft. For example, one researcher noted that organizations could encrypt data or use tokens so static account numbers could not be used on their own. There is no single solution to address all risks of harm, based on our review of documentation and the views of academic, consumer, government, and industry experts.

²⁹See GAO, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in the Technology and the Marketplace*, [GAO-13-663](#) (Washington, D.C.: Sept. 25, 2013); and *Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data*, [GAO-06-674](#) (Washington, D.C.: June 26, 2006).

³⁰Facial recognition technology is one of several biometric technologies that identify individuals by measuring and analyzing their physiological or behavioral characteristics.

Consumers Can Use Free Credit Freezes and Fraud Alerts to Effectively Prevent New-Account Fraud

A credit freeze is the only consumer option that can prevent one type of identity theft-related fraud, and recent federal legislation made credit freezes free and easier to place or lift. This option is effective because it restricts potential creditors from accessing a consumer's credit report to open a new account until the consumer asks the nationwide consumer reporting agency to remove or temporarily lift the freeze. In contrast, identity theft services and self-monitoring detect or remediate identity theft after it has occurred, but do not prevent the fraud from occurring in the first place. We interviewed representatives, or reviewed the consumer education or informational materials, of consumer, industry, and government entities and found that almost all of them included credit freezes on credit reports as a useful consumer option to protect against identity theft.

More specifically, the Economic Growth, Regulatory Relief, and Consumer Protection Act, which took effect on September 21, 2018, required the three nationwide consumer reporting agencies (Equifax, Experian, and TransUnion) to make placing and lifting freezes free and specifies that the agencies must place a freeze within 1 business day, and lift it within 1 hour, of receiving a telephone or electronic request (see fig. 1).³¹ Consumers must contact each of the three agencies individually and request the freeze. Consumers obtain a PIN from each company, which enables them to lift or remove a freeze at a later date. Before the 2018 act, consumers typically had to pay \$5-\$10 per agency to place a credit freeze. Some experts had noted cost and inconvenience as some of the limitations to a credit freeze. The new law addresses these concerns to some degree by making credit freezes free and requiring these consumer reporting agencies to lift freezes expeditiously on request.

³¹ See Pub. L. No. 115-174, §301, 132 Stat. 1296, 1326 (2018) (codified at 15 U.S.C. § 1681c-1(i)). The Congressional Budget Office estimated that about 0.3 percent of Americans with credit reports have frozen their credit. Congressional Budget Office, *Congressional Budget Office Cost Estimate, S. 2155, Economic Growth, Regulatory Relief, and Consumer Protection Act* (Washington, D.C.: March 5, 2018).

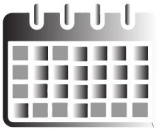
Figure 1: Overview of Credit Freezes

Selected 2018 Federal Legislative Changes



Free Credit Freezes

- Individuals can place freezes on their credit reports for **free** at the three nationwide consumer reporting agencies—Equifax, Experian, and TransUnion.



Freeze within 1 Business Day

- Consumer reporting agency must place the freeze within **1 business day** of receiving a phone or electronic request (or within **3 business days** of a mailed request).



Unfreeze within 1 Hour

- Consumer reporting agency must remove a freeze within **1 hour** of receiving a phone or electronic request (or within **3 business days** of a mailed request).

Why Credit Freezes Can Be Helpful:

- Prevents new accounts from being opened, in situations where review of a credit report is required.
- Guardians can place credit freezes for minor children (under age 16) or adults who are incapacitated.
- Cited by experts as one of the most effective tools for preventing new-account fraud.
- Relatively convenient: freezes can be managed electronically (or through other methods) and can be removed temporarily for a specified duration.

Consumers Should Be Aware:

- Consumers must request a freeze at each of the three agencies separately.
- Could still cause delays in approval of loans or other credit applications, especially if consumer forgets or loses the personal information number (PIN) the agencies give to consumers to unfreeze their credit reports.
- Freezes do not prevent fraud on existing accounts (for example, the use of a stolen credit card number to make charges on a credit card).
- Does not prevent other types of harm, such as tax refund or medical identity fraud.
- Not all access to credit reports is frozen (for example, still allowed for insurance underwriting and employment background checks).
- Credit reports at agencies other than Equifax, Experian, and TransUnion will not be frozen (for example, those used to open utility accounts).

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

While the new law removed some barriers to placing credit freezes, others still exist and the freezes have some limitations. For example, consumers still have to lift a freeze before applying for a loan or new credit account and need to place or remove a freeze at each consumer reporting agency separately, which could cause delays for consumers actively shopping for a home, car, or other purchase requiring the extension of credit. Two consumer groups said that there is confusion about how the law would affect minor children. (Under the new law, credit freezes only can be placed on behalf of children under age 16, but not minors ages 16 and 17—who must place freezes themselves).

Moreover, as the new law only applies to the three nationwide consumer reporting agencies, credit freezes do not protect against new-account fraud resulting from the use of credit reports from other consumer reporting agencies. For example, one consumer group recommended that consumers place a fourth freeze with the National Consumer Telecom and Utilities Exchange—a consumer reporting agency that maintains credit reports that telecommunications or utilities companies may use to check the creditworthiness of consumers interested in opening phone or utility accounts. The law also permits insurance companies and employers to continue to access credit reports even after they are frozen, among other exceptions.

One general limitation of credit freezes is that they do not protect against new-account fraud in cases in which credit reports are not used to verify a consumer's creditworthiness. Furthermore, credit freezes do not protect against existing-account fraud, such as fraudulent credit card charges, or certain other types of fraud, such as identity theft tax refund fraud or synthetic identity fraud using elements of individuals' identity information.

While experts with whom we spoke across industry, government, and consumer groups generally believed credit freezes to be an effective tool in preventing new-account fraud, some consumer and industry experts indicated that fraud alerts also can be a good alternative for consumers. Unlike a credit freeze, a fraud alert still allows companies to access an individual's credit report for the purpose of opening a loan or credit account. Fraud alerts notify companies requesting the reports that the individual may have been a victim of identity theft. The alerts require companies to verify consumers' identities before they issue credit to a

consumer.³² Fraud alerts therefore can make it harder for an identity thief to open accounts in a consumer's name. Moreover, fraud alerts are easier to place than credit freezes, as consumers only need to contact one of the three nationwide consumer reporting agencies to place a fraud alert (that agency is then obligated to contact the other two on the individual's behalf). The Economic Growth, Regulatory Relief, and Consumer Protection Act extended the period of an initial fraud alert from 90 days to 1 year.³³

However, fraud alerts do not restrict access to consumers' credit reports the way freezes do. Therefore, some consumer group and industry representatives noted that consumers should be aware that a fraud alert may not offer as strong a protection as a credit freeze does. We did not find any data or analysis on the effectiveness of fraud alerts compared to credit freezes or monitoring options. One consumer group told us that it recommends that after a data breach consumers first place a fraud alert, because it requires contacting only one of the three nationwide consumer reporting agencies, and then follow up by placing a credit freeze at the three agencies.

The three nationwide consumer reporting agencies also offer a product called a credit lock that is functionally similar to a credit freeze in that it restricts access to an individual's credit report. Credit locks do not require consumers to use a PIN and consumers can turn access to credit reports on or off through an application on their mobile phone. However, credit locks are not subject to the same federal requirements regarding the placement and removal of freezes and therefore do not offer the same

³²See 15 U.S.C. § 1681c-1(h)(1)(B). Consumers can request an initial fraud alert, extended fraud alert, or active duty alert at no cost with any one of the three nationwide consumer reporting agencies, which automatically must notify the other two. See 15 U.S.C. § 1681c-1(a)-(c). An initial fraud alert stays on the victim's credit file for 1 year after which the consumer may place another fraud alert. An extended fraud alert, which lasts for 7 years, is available to victims of identity theft who have filed a formal identity theft report with one of the three agencies. Active duty alerts, which last for 1 year, are available to deployed military service members.

³³See Pub. L. No. 115-174, §301(a)(1), 132 Stat. 1296, 1326 (2018) (codified at 15 U.S.C. § 1681c-1(a)(1)(a)). Additionally, the act mandated that FTC issue a rule regarding the law's requirement that the nationwide consumer reporting agencies provide a free electronic credit monitoring service that would notify active-duty military members within 24 hours of any "material" additions or modifications to their credit files. § 302(d)(1).

degree of protection to consumers.³⁴ Instead, credit locks are private products subject to the consumer reporting agencies' terms and conditions, which could change. A credit lock is in place only as long as the individual subscribes to an agency's service, but a credit freeze remains in place until the consumer chooses to remove it. Finally, consumers may be charged a fee to place a credit lock, whereas credit freezes can now be placed for free.

Factors Consumers Can Consider When Assessing Options after Data Breaches

Based on our interviews and review of consumer education materials and our 2017 report, we identified four factors that consumers can consider in deciding which options are best for them in responding to a breach of their personal information:

- **Prevention.** Consumers can consider the extent to which an option might prevent fraud. For example, because credit freezes block all access to an individual's credit report, by definition they are effective in preventing new-account fraud where credit reports are used as part of the account-opening process. Identity theft services do not prevent fraud, but detect suspicious activity or help restore identities after identity theft.
- **Cost.** Consumers can consider the cost of a service. For instance, consumers can consider whether to pay for commercial identity theft services if they believe the value of the service outweighs the effort of monitoring their accounts on their own. In addition, they may consider that credit freezes now are available for free.
- **Convenience.** Consumers may consider the convenience of a service. For example, while consumers can monitor their own credit reports and accounts, some might prefer not to or may be limited in their ability to do so. In addition, technologies offered through financial institutions that automatically alert customers to any transactions

³⁴The Fair Credit Reporting Act protects the accuracy and confidentiality of personal information collected or used for eligibility determinations for such purposes as credit, insurance, or employment. As such, it regulates the collection and use of consumers' personal information by consumer reporting agencies. Moreover, the Fair Credit Reporting Act requires information on credit freezes to be included in any notice of consumer rights required under the act. See 15 U.S.C. § 1681c-1(i)(5).

involving their accounts can be a convenient, no-cost way for consumers to monitor their accounts.

- **Type of information at risk.** Finally, several experts from consumer and industry organizations indicated that the type of option that might be beneficial would depend on the type of information at risk. For example, one consumer group representative noted that if a credit card number were stolen, an identity monitoring service that monitored the dark web for Social Security numbers might not be needed. Furthermore, consumers should consider that credit monitoring will be of limited effectiveness in alerting them to misuse of an existing credit account—which is more common than fraud related to setting up new accounts.³⁵ For more information on consumers' options, see appendix II.

Federal Agencies Provide Assistance to Consumers Affected by Data Breaches and Identity Theft

Among federal agencies, FTC serves as a primary source for free assistance (including online resources, educational outreach, and customized assistance through IdentityTheft.gov) to consumers on ways to respond to data breaches, identity theft, and related harm. Approximately 13 percent of those affected by the 2015 OPM breaches used credit and identity monitoring and identity restoration services that OPM offered them and a fraction of a percent made identity theft insurance claims (the payouts for which averaged \$1,800). Data we assessed for this report support a 2017 recommendation we made to the Office of Management and Budget (OMB) to revise guidance to federal agencies about responding to data breaches and one to Congress to consider permitting agencies to determine appropriate levels of identity theft insurance offered after data breaches.

³⁵As noted previously, for 85 percent of identity-theft victims in 2016, the most recent incident involved misuse or attempted misuse of one type of existing account, such as a credit card or bank account. Only 1 percent of those 16 or older experienced the opening of a new account or other misuse of personal information apart from misuse of an existing account. See Department of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2016* (January 2019).

FTC Is Primary Provider of Federal Assistance to Consumers Affected by Data Breaches and Identity Theft

Federal Trade Commission

FTC, as a primary source for assistance to consumers on issues related to data breaches and identity theft, provides guidance and assistance through its website and through conferences and workshops.³⁶

Online and printed resources. FTC's home page includes links to identity theft-related resources, including information about key options consumers can consider to help them mitigate identity theft risks and other harms, and a link to IdentityTheft.gov (discussed later in this section). FTC updates the information regularly, such as after large-scale data breaches.

Outreach. FTC maintains relationships with state government, law enforcement, and community and consumer organizations, through which it conducts outreach about how to respond to exposure or loss of personal information and identity theft mitigation. For example, FTC collaborated with the International Association of the Chiefs of Police to update the association's model policy for identity theft to include referral information for IdentityTheft.gov. FTC also has held webinars, conferences, and workshops on topics related to data breaches and identity theft for groups including government officials, nonprofits, and the general public.

³⁶The Identity Theft and Assumption Deterrence Act of 1998 establishes FTC as the central clearinghouse for identity theft victim complaints and directs FTC to provide consumer education to identity theft victims. See Pub. L. No. 105-318, § 5(a), 112 Stat. 3007, 3010 (codified at 18 U.S.C. § 1028 note). More recently, an Executive Order included a provision calling for federal agencies to centralize identity theft information and resources at FTC's website, IdentityTheft.gov, and through the general FTC website. Exec. Order No. 13681, 78 Fed. Reg. 63491, 63492 (Oct. 23, 2014). FTC's primary legal authority comes from section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive acts or practices in the marketplace. See 15 U.S.C. § 45. FTC has authority to enforce sector-specific laws, including the Truth in Lending Act, the CAN-SPAM Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act. As directed by Congress, FTC also has authority to issue rules that regulate specific areas of consumer privacy and security. For example, FTC's Red Flags Rule requires financial institutions and certain creditors to have programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.

Customized assistance (IdentityTheft.gov). FTC provides information and customized assistance through IdentityTheft.gov to individuals whose information was lost or stolen or who experienced identity theft or other harm, such as tax refund fraud. During fiscal year 2018, IdentityTheft.gov received almost 2 million unique visitors. The website in its current form has been in place since January 2016 and offers the following types of assistance:

- **Steps to take after identity theft.** IdentityTheft.gov provides individual victims with step-by-step instructions to resolve specific problems. From January 2016 (when FTC launched the current version of IdentityTheft.gov) through October 1, 2018, approximately 700,000 individuals set up and activated accounts on the website to help them recover from identity theft. Individuals who set up accounts can indicate what kind of information was stolen and what kind of adverse event they experienced. The site helps users generate pre-filled letters, affidavits, and forms to send to consumer reporting agencies, businesses, debt collectors, and IRS, as appropriate. For example, individuals who fill out an Identity Theft Report affidavit can use this report instead of filing a police report to request extended 7-year fraud alerts (available to identity theft victims) on their credit reports. In addition, individuals who experienced tax refund fraud can fill out a form on IdentityTheft.gov that is then submitted directly to IRS. An individual who experienced credit card fraud would be advised to take different steps than one who experienced fraud related to utility bills or medical insurance.
- **Steps to take after data breaches or loss of personal information.** IdentityTheft.gov/databreach provides checklists and suggestions for people whose personal information was lost or exposed but has not yet been misused.

FTC also maintains an online chat function and telephone number for those who need additional assistance. For complex cases, FTC staff may refer individuals to the Identity Theft Resource Center, a nonprofit organization.

We found that in developing and updating the website, FTC followed some key practices for consumer education planning.³⁷ One key practice we identified was consulting with stakeholders. According to FTC staff we

³⁷In [GAO-08-43](#), we describe key practices for conducting consumer education identified by an expert panel that we convened.

interviewed and documentation we reviewed, FTC obtained feedback from stakeholders such as law enforcement agencies and community organizations in developing IdentityTheft.gov. Another key practice we identified was assessing users' needs. FTC conducted usability testing to ensure the site's features were easy to use. FTC staff also told us that after receiving user feedback, they made it easier for users to set up an account. FTC also made changes to IdentityTheft.gov—such as incorporating the ability to auto-generate forms—to implement a 2014 Executive Order calling for federal agencies to centralize identity theft information at the website.³⁸ Furthermore, in January 2018, FTC implemented a new function that allows users who report identity theft tax refund fraud to file reports directly with IRS. Since its launch in early 2018 through October 1, 2018, almost 22,000 IRS Identity Theft Affidavits (IRS Form 14039) were submitted to IRS through IdentityTheft.gov. In general, experts across consumer, government, and industry organizations and identity theft service providers we interviewed expressed the view that IdentityTheft.gov is a valuable or user-friendly resource.

Other Federal Agency Resources

Other federal agencies provide assistance to consumers on topics related to identity theft, including CFPB, the Department of Justice, IRS, and the Social Security Administration.³⁹

CFPB. CFPB enforces, supervises for compliance with, and issues regulations to implement the federal consumer financial laws that address certain firms' and financial institutions' practices, which may include data security. A few of these laws and regulations contain provisions that can

³⁸Exec. Order No. 13681, 78 Fed. Reg. 63491 (Oct. 23, 2014).

³⁹For example, see Department of Justice, Identity Theft, <https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud>, which we accessed on November 19, 2018. Also see Internal Revenue Service, *Taxpayer Guide to Identity Theft*, <https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft>, accessed on November 19, 2018; *Data Breach: Tax-Related Information for Taxpayers*, May 2018; and *Identity Protection: Prevention, Detection, and Victim Assistance*, July 2018. See Social Security Administration, *Identity Theft and Your Social Security Number*. These agencies were outside the scope of our review for this report, but we previously reported on some related topics (for instance, see [GAO-18-418](#)).

help protect the personal information of consumers.⁴⁰ CFPB also offers consumer education resources.

Similarly to FTC, CFPB included information about how consumers can address risks related to exposure of personal information and recover from identity theft in the bureau's overall consumer education activities. CFPB provides consumer education materials related to data breaches and identity theft through its blog and its financial education resource, "Ask CFPB." CFPB also maintains relationships with external groups, such as librarian networks. CFPB provides links to FTC resources about data breaches and identity theft topics on its website, so as not to duplicate efforts, according to CFPB staff.⁴¹ The two agencies also have coordinated some efforts. FTC and CFPB published a jointly produced blog post on September 21, 2018, the date the new free credit freeze and 1-year fraud alert provisions took effect. Such coordination is consistent with the 2014 Executive Order, which designated FTC as a centralized source of information about identity theft across the federal government.

Staff of both agencies said that in developing new resources, they monitor information from a variety of sources, including consumer complaints, news and social media, and reports from other government entities, law enforcement, or nongovernmental stakeholders.

Other federal and state agencies. IRS and the Social Security Administration provide some assistance to consumers for specific types of identity theft. For example, as noted previously, IRS provides some taxpayers with PINs if they are victims of identity theft tax refund fraud. In addition, states enforce laws and regulations and provide consumer education resources and assistance to consumers at risk of identity theft

⁴⁰These include sections 502 through 509 of the Gramm-Leach Bliley Act, sections 1031 and 1036 of the Dodd-Frank Wall Street Reform and Consumer Protection Act concerning unfair, deceptive, or abusive acts and practices, the Fair Credit Reporting Act, and the Fair Debt Collection Practices Act. See Pub. L. No. 111-203, § 1002(12), 124 Stat. 1376, 1957 (2010) (codified at 12 U.S.C. § 5481(12)). CFPB has no authority under section 501(b) of the Gramm-Leach Bliley Act, which required FTC and other agencies (but not CFPB) to establish standards for financial institutions on administrative, technical, and physical safeguards to ensure the security and confidentiality of customer records and information, to protect against anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer. See 15 U.S.C. § 6801(b).

⁴¹Other federal agencies' websites also provide links to FTC resources, including those of OPM, IRS, the Department of Justice, and the Social Security Administration.

and other harms as a result of data breaches. For example, the Illinois Attorney General's office maintains a call-in number for victims of identity theft, and the Colorado Bureau of Investigation can assist residents with identity theft issues.

Few People Used Identity Theft Services OPM Provided, Very Few Made Insurance Claims, and Payouts Received Were Low

OPM offered identity theft services to approximately 22.1 million individuals whose personal information was compromised during the 2015 data breaches at OPM.⁴² Personnel records or OPM systems containing information from the background investigations of current, former, and prospective federal employees and other individuals were breached. The services, offered at no cost to affected individuals, included credit monitoring, identity monitoring, identity restoration services, and identity theft insurance.⁴³ To receive credit and identity monitoring services, affected people have to enroll with the identity theft service provider with which OPM contracted, but identity theft insurance and identity theft restoration services are available to the entire affected population whether or not they enroll.

Few affected individuals have used the services. According to data from OPM, as of September 30, 2018, close to 3 million, or 13 percent, of individuals affected by the 2015 incidents had made use of the services. As seen in figure 2, the great majority of enrollments occurred in the months immediately following notification of the breach.⁴⁴ OPM staff said that the spike in enrollments in July and August 2016 likely was due to the follow-up mailing that OPM sent to approximately 10 percent of affected

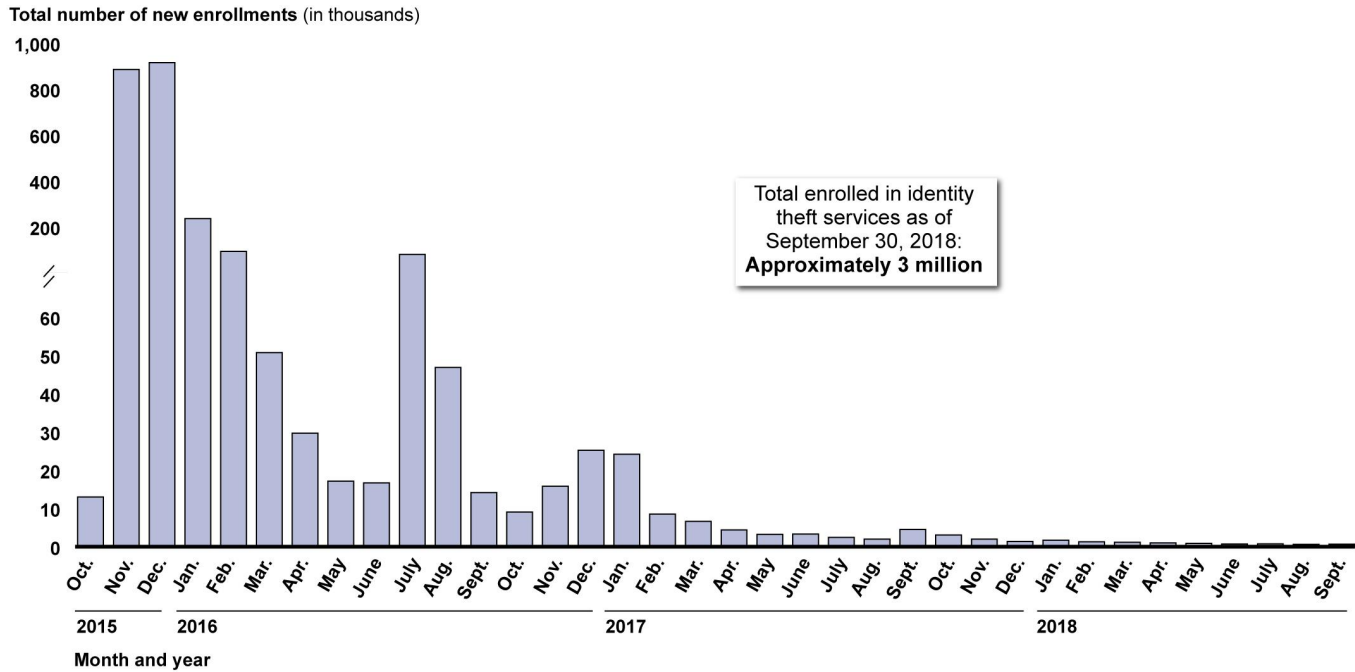
⁴²The federal contracts awarded in 2015 for the OPM data breaches provided for federal agencies to receive information about the identity theft services delivered by contractors, such as information about call-center wait times and the number and status of identity restoration cases.

⁴³The identity restoration and insurance provided to consumers covers all incidents of identity theft that occur during the coverage period, regardless of the source.

⁴⁴OPM data show that of the approximately 3 million individuals enrolled in identity theft services through September 30, 2018, there were about 2.7 million adults and 350,000 minors. See [GAO-17-254](#) for more information.

individuals whose mailing addresses were incorrect in the original mailing of notifications.⁴⁵

Figure 2: Enrollment in Identity Theft Services Offered by Office of Personnel Management, October 2015–September 2018



Source: GAO analysis of Office of Personnel Management data. | GAO-19-230

Notes: The Office of Personnel Management (OPM) offered identity theft services to approximately 22.1 million individuals whose sensitive personal information was compromised during the 2015 data breaches of OPM personnel records or OPM systems containing information from the background investigations of current, former, and prospective federal employees and other individuals. The services included credit and identity monitoring, identity restoration services, and identity theft insurance. According to OPM staff, the spike in enrollments in July and August of 2016 likely was due to the follow-up mailing that OPM sent to approximately 10 percent of affected individuals whose mailing addresses were incorrect in the original September 2015 notification.

In addition, according to OPM-reported data we reviewed, of the 3 million individuals who used the services, about 1 percent made identity restoration requests and a fraction of 1 percent submitted insurance claims. According to data we reviewed, approximately 27,000 identity restoration cases had been resolved as of September 30, 2018. In

⁴⁵OPM worked with the Department of Defense and a commercial address validation service to identify the correct addresses and sent out notifications to these individuals in June 2016.

addition, 61 insurance claims (of 81 submitted) had been paid, totaling \$112,000, with an average payout of \$1,800.⁴⁶

Since 2015, OPM has obligated approximately \$421 million for identity theft services and as of November 30, 2018, OPM paid out approximately \$361 million of the obligated funds.⁴⁷ OPM is required to provide identity theft services through September 2026.⁴⁸ The contract to provide these services on behalf of OPM expired in December 2018; OPM re-competed and awarded a single contract that month to ID Experts, the company that had been providing these services.⁴⁹

After the OPM breaches in 2015, OPM provided federal employees and other affected individuals with information and guidance about their options in mailed letters and on its website. On its website, OPM developed a Cybersecurity Resource Center and included background about the breaches and who was affected; instructions for how to enroll in identity theft services; and a Frequently Asked Questions webpage that included links to FTC resources, including IdentityTheft.gov. OMB's 2017 policy guidance to federal agencies, including OPM, states that agencies should determine appropriate information to provide to affected individuals and review breach responses annually. Consistent with that guidance, OPM's September 2017 Breach Response Plan calls for the agency to review its breach response plan annually, including to reinforce or improve training and awareness. In December 2018, OPM updated its

⁴⁶As stated previously, all incidents are covered regardless of the source.

⁴⁷In [GAO-17-254](#), we found that OPM's breach-response policies and procedures did not specifically address identity theft services, which could hinder informed decision-making by the agency on the appropriate services, if any, to offer affected individuals. Therefore, we recommended that OPM incorporate criteria and procedures for determining whether to offer identity theft services into the agency's policy on responding to data breaches. We also found that OPM had not adequately documented how it made its decisions about its 2015 breaches. We recommended that the agency implement procedures to help assure that significant decisions on the use of identity theft services would be appropriately documented. In September 2017, OPM implemented both recommendations.

⁴⁸See Consolidated Appropriations Act, 2017, Pub. L. No. 115-31, § 633, 131 Stat. 135, 376.

⁴⁹According to OPM staff, the contract was competed through a blanket purchase agreement bidding process. A blanket purchase agreement is a contracting vehicle that agencies are encouraged to use in order to easily access and acquire qualified providers on prenegotiated prices for services. The General Services Administration has established an identity theft services blanket purchase agreement, which includes selected identity theft service providers.

website to incorporate changes in the cost of credit freezes and duration of fraud alerts resulting from new legislation we discussed earlier.

OMB Has Not Revised Post-Data Breach Guidance to Agencies and Insurance Coverage Amount for Identity Theft Insurance Remains High

Data we assessed for this report support a 2017 recommendation we made to OMB and a matter for congressional consideration, both of which have not yet been implemented.⁵⁰ In our March 2017 report, we found that OMB policy guidance for federal agencies on how to prepare for and respond to data breaches did not address how agencies might assess the effectiveness of identity theft services relative to lower-cost alternatives.⁵¹ For example, the guidance did not discuss whether identity theft services would be preferable to alternatives (such as fraud alerts, credit freezes, or the agency conducting its own database monitoring). We concluded that the guidance might not fully reflect the most useful and cost-effective options agencies should consider in response to a breach—contrary to OMB’s risk-management and internal control guidance calling on federal leaders to improve effectiveness and efficiency. Therefore, we recommended that OMB conduct an analysis of the effectiveness of identity theft services relative to alternatives, and revise its guidance to federal agencies in light of the analysis. In oral comments on a draft of the 2017 report, staff from OMB’s Office of Information and Regulatory Affairs said that our draft recommendation to OMB on expanding OMB’s guidance to federal agencies would benefit from greater specificity, and we revised this recommendation to provide greater clarity.

We contacted OMB several times between May 2018 and early March 2019 to update the status of this recommendation but as of March 2019,

⁵⁰See [GAO-17-254](#).

⁵¹OMB Memorandum M-17-12. In this memorandum, OMB defines personally identifiable information as information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information linked or linkable to a specific individual. OMB was directed to update this guidance by the October 2015 Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government. See Office of Management and Budget, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*, M-16-04 (Washington, D.C.: Oct. 30, 2015).

OMB had not responded with an update.⁵² In our current review, we found that information on the effectiveness of various consumer options continues to be limited. We also found that some free and low-cost alternatives to free or fee-based identity theft services can prevent or more directly address new account fraud and some options consumers can take on their own have become less burdensome. Therefore, we stand by this recommendation.

In addition, as noted previously in this report, the identity theft insurance that OPM offered to affected individuals resulted in few insurance claims, and the amounts claimed have been small. These data are consistent with the findings of our 2017 report—which reported that the number and dollar amount of claims for identity theft generally were low.⁵³ They also reinforce our conclusion that the \$5 million per-person coverage limit mandated by Congress likely was unnecessary and might impose costs without providing a meaningful corresponding benefit. Specifically, we noted that \$5 million in coverage would increase federal costs unnecessarily, likely mislead consumers about the benefit of the product, and create unwarranted escalation of coverage amounts in the marketplace.

Therefore, we reiterate the matter for congressional consideration we made in our March 2017 report: in the event that Congress again requires an agency to provide individuals with identity theft insurance in response to a breach, it should consider permitting the agency to determine the appropriate level of that insurance.

⁵²[GAO-17-254](#) also recommended that OMB explore options to address the risk of duplication in federal provision of identity theft services in response to data breaches, and take action if viable options were identified. In November 2018, OMB staff told us this recommendation would be updated as part of OMB's response to our request for the status of recommendations in our annual report on opportunities to reduce fragmentation, overlap, and duplication, reduce costs, and increase revenue, for the government. See *GAO, 2018 Annual Report: Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits*, [GAO-18-371SP](#) (Washington, D.C.: Apr. 26, 2018).

⁵³[GAO-17-254](#). We found identity theft insurance is limited in covering direct financial losses—that is, money that was stolen. Instead, the insurance generally reimburses consumers for out-of-pocket expenses they incur related to the process of restoring their identity and credit records. While the overall coverage limit for policies can be quite high (around one million dollars), the process of resolving identity theft typically does not require significant expenses, according to many providers with which we spoke and two consumer groups.

Agency Comments

We provided a draft of this report to CFPB, FTC, and OPM. The agencies provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Director of CFPB, the Chair of FTC, and the Acting Director of OPM. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions concerning this report, please contact me at (202) 512-8678 or ortiza@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.



Anna Maria Ortiz
Acting Director, Financial Markets and Community Investment

Appendix I: Objectives, Scope, and Methodology

This report examines (1) information and expert views about the effectiveness of options consumers can use to prevent or address the risks resulting from data breaches; and (2) federal assistance available to help consumers understand these options, including the status of one matter for congressional consideration and one recommendation relating to these issues in our 2017 report.¹

To address the first objective, we conducted a literature review to identify any studies or independent research on the effectiveness of various options consumers have for mitigating data breach harms, consumer attitudes and behavior following data breaches, and identity theft and other harm to individuals from exposure of personal information. We searched databases of scholarly publications and other sources for work generally published within the last 5 years. Examples of databases searched include ProQuest, EconLit, Policy File Index, and SciTech Premium Collection. We searched for terms including “effective,” “data breach,” “identity theft,” “consumer attitudes,” and “consumer behavior” and options such as “credit freeze,” “fraud alert,” and “credit lock.” We also reviewed relevant academic literature to identify additional studies. From these searches, we did not identify any studies that assessed the extent to which commercial identity theft services were effective in preventing or mitigating harm from exposure of personal information. We identified and reviewed 54 studies that appeared in peer-reviewed journals or research institutions’ publications and were relevant to consumer attitudes and behavior related to privacy, data breaches, and identity theft.

To ensure the selection of a range of perspectives on the effectiveness of options to mitigate harms, we reviewed the selection of experts and sources in our prior report and our literature review, and updated that selection through additional searches and recommendations from discussions with experts and identity theft service providers and review of

¹See GAO, *Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud*, [GAO-17-254](#) (Washington, D.C.: Mar. 30, 2017).

relevant literature. We defined experts as those representing consumer and industry policy organizations that have conducted research or taken policy positions on consumers' or entities' options after data breaches; academics who conducted research on relevant topics; and federal and state government staff with specific positions of responsibility in consumer protection or education. We also contacted seven companies that provide identity theft services to consumers.

We interviewed representatives of a nongeneralizable sample of 35 entities in the following categories: academic or independent research institution (4); consumer or privacy research and advocacy (10); industry association, identity theft service provider, or industry consultant (12); and federal or state government (9). We also reviewed relevant consumer education and other materials produced by consumer, government, industry, and other entities. We interviewed academics from Carnegie-Mellon University, RAND Corporation, the University of Maryland, and the University of Rochester. In addition, we interviewed representatives from the following organizations:

- **Consumer or privacy groups:** AARP, Consumer Action, Consumer Federation of America, Consumer Reports, Electronic Privacy Information Center, Identity Theft Resource Center, National Consumer Law Center, Privacy Rights Clearinghouse, U.S. PIRG, and World Privacy Forum.
- **Industry associations or consultants:** American Bankers Association, Consumer Data Industry Association, Property and Casualty Insurers Association of America, National Retail Federation, and Rational 360.
- **Identity theft service providers:** Credit Karma, Equifax, Experian, ID Experts, ID Shield, LifeLock, and TransUnion.²
- **Government agencies:** Consumer Financial Protection Bureau (CFPB), Federal Reserve Bank of Philadelphia, Federal Trade Commission (FTC), Office of Personnel Management (OPM), and Offices of the Attorney General of California, Connecticut, Illinois, Massachusetts, and New York.³

²We also reviewed the website of Credit Sesame.

³We also reviewed the websites of the Offices of the Attorney General of Florida, Indiana, and Texas and of the Colorado Office of Victims Services.

Throughout this report, we use certain qualifiers when describing responses from interview participants and views of entities whose articles and written material we reviewed, such as “few,” “some,” and “most.” We define few as a small number such as two or three. The specific quantification of categories depends on the overall numbers of entities that addressed a specific topic. For example, we may refer to views shared by a proportion of the 10 consumer groups we interviewed, or those shared by identity theft service providers.

We also reviewed provisions in the Economic Growth, Regulatory Relief, and Consumer Protection Act, enacted in May 2018, that address credit freezes and fraud alerts (two tools for preventing new-account fraud).⁴

To address the second objective, we reviewed and analyzed documentation and interviewed staff from FTC, CFPB, and OPM. We reviewed and analyzed FTC, CFPB, and OPM consumer education materials including blog posts, online fact sheets, and printed brochures and data on usage of the materials. For example, we analyzed FTC, CFPB, and OPM data and website analytics for their data breach- and identity theft-related web pages. We interviewed FTC and CFPB agency staff about their assistance to individuals and how they measure effectiveness of their efforts. We reviewed documentation and interviewed agency staff about the development, implementation, and assessment of consumer education materials and other resources and assistance. For example, we reviewed materials documenting FTC’s outreach to stakeholders and usability testing of IdentityTheft.gov. We compared the activities against a 2014 Executive Order on the security of consumer financial transactions, key practices for consumer education planning we identified in prior work, and federal standards for internal control.⁵

We analyzed data from the company with which OPM contracted to provide identity theft services to the approximately 22.1 million individuals whose information was exposed in the 2015 data breaches. We obtained

⁴Pub. L. No. 115-174, § 301(a), 132 Stat. 1296, 1326 (2018) (codified at 15 U.S.C. § 1681c–1(i)).

⁵Exec. Order No. 13681 79 Fed. Reg. 63491 (Oct. 23, 2014). See GAO, *Digital Television Transition: Increased Federal Planning and Risk Management Could Further Facilitate the DTV Transition*, [GAO-08-43](#) (Washington, D.C.: Nov. 19, 2007); and *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014). Also see Office of Management and Budget, *Preparing for and Responding to a Breach of Personally Identifiable Information*, M-17-12 (Washington, D.C.: Jan. 3, 2017).

data on the number of enrollments, the number and size of identity theft insurance claims submitted and paid, and number of identity restoration cases the companies handled. We assessed the reliability of the data by interviewing agency officials and reviewing documentation about the systems used to store the data. We found the data to be reliable for purposes of this reporting objective. We also reviewed the online guidance OPM provided to affected individuals and assessed the guidance against Office of Management and Budget guidance for agencies following data breaches and OPM's 2017 Breach Response plan.

In addition, for both objectives, we reviewed the evidence gathered and analyzed for the 2017 GAO report ([GAO-17-254](#)) and updated the status of the matter for congressional consideration and recommendations made in that report.⁶

We conducted this performance audit from November 2017 to March 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.




⁶See GAO, *Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud*, [GAO-17-254](#) (Washington, D.C.: Mar. 30, 2017).

Appendix II: What Can Consumers Do After a Data Breach?

Figure 3 below provides information on actions consumers can take to monitor for identity theft or other forms of fraud, protect their personal information, and respond if they have been a victim of identity theft. This information summarizes prior GAO work and comments of academic, consumer organization, industry, and government experts.¹

¹GAO, *Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud*, [GAO-17-254](#) (Washington, D.C.: Mar. 30, 2017).




Figure 3: What Can Consumers Do After a Data Breach?

Prevent Fraud on New Credit Accounts 		
Consumer Option	How This Option Can Help	Consumers Should Be Aware
 <p>Place a credit freeze on credit reports at Equifax, Experian, and TransUnion—the three nationwide consumer reporting agencies.</p>	<ul style="list-style-type: none"> • Prevents identity thieves from opening new credit accounts in an individual’s name—where credit reports are required. • Guardians can place credit freezes for minor children (under age 16) or adults who are incapacitated. 	<ul style="list-style-type: none"> • Consumers must request a freeze at each of the three agencies separately. • Could still cause delays in approval of loans or other credit applications, especially if consumer forgets or loses the personal information number (PIN) the agencies give to consumers to unfreeze their credit reports. • Freezes do not prevent fraud on existing accounts (for example, the use of a stolen credit card number to make charges on a credit card). • Freezes do not prevent other types of harm, such as tax refund or medical identity fraud. • Not all access to credit reports is frozen (for example, still allowed for insurance underwriting and employment background checks). • Credit reports at agencies other than Equifax, Experian, and TransUnion will not be frozen (for example, those used to open utility accounts).
 <p>Place a fraud alert at the three nationwide consumer reporting agencies, which lasts 1 year and can be renewed.</p>	<ul style="list-style-type: none"> • Fraud alerts let businesses know that a consumer may have been a victim of fraud. • Businesses must take extra steps to verify the identity of the individual seeking to open accounts. • Members of the military can place active duty alerts. 	<ul style="list-style-type: none"> • Consumers can request a fraud alert at one of the three agencies and this agency must notify the other two to place the alert. • Victims of identity theft can place extended fraud alerts that last for 7 years. • Fraud alerts still allow access to credit reports. • Businesses that do not use the three agencies will not see the alert.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

Monitor for Some Types of Fraud on Financial Accounts



Consumer Option	How This Option Can Help	Consumers Should Be Aware
 <p>Review free credit reports every 12 months (from Equifax, Experian, and TransUnion) at annualcreditreport.com.</p>	<ul style="list-style-type: none"> • Can help consumers spot suspicious activity or fraud involving credit accounts. 	<ul style="list-style-type: none"> • Consumers can check one of the three reports every 4 months to improve chances of catching problems throughout the year.
 <p>Review bank and other financial account statements regularly or set up free automatic alerts.</p>	<ul style="list-style-type: none"> • Can alert consumers to suspicious activity on their accounts. 	<ul style="list-style-type: none"> • The availability and features of alerts may vary among financial institutions.
 <p>Consider enrolling in credit or identity monitoring services.</p>	<ul style="list-style-type: none"> • Credit monitoring can alert consumers after the fact that someone may have used their personal information to open a credit account (take out a loan or sign up for a credit card). • Identity monitoring can alert consumers of misuse of personal information or appearance of their information on illicit websites (the “dark web”). 	<ul style="list-style-type: none"> • These services do not directly address risks of medical identity theft, identity theft tax refund fraud, or government benefits fraud. • Credit monitoring can spot fraud but generally cannot prevent it, and does not identify fraud on existing or noncredit accounts. • Identity monitoring also cannot prevent fraud. • It is unclear what actions consumers can take once alerted that their information appears on the dark web other than continuing to monitor their accounts. • These services may be part of a package of identity theft services, including restoration services, or identity theft insurance. • Free services that entities that have experienced data breaches may offer to affected consumers vary in the type and level of service and may only last for 1-2 years. Risks can exist for much longer. • Paid services typically cost \$5–\$30 a month.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

Monitor for Other Types of Identity Theft or Fraud



Consumer Option

How This Option Can Help

Consumers Should Be Aware



Mobile Phone or Utility Account Fraud

Review mobile phone and utility bills regularly.

- Can spot suspicious activity on existing accounts.

- Consumers with credit freezes may need to lift them before applying for new utility or phone accounts.



Medical Identity Theft

Review medical bills and health insurance explanations of benefits.

- Can spot suspicious activity, such as bills or insurance claims for services consumers did not receive.

- Consumers who spot problems can contact fraud departments at health insurers.



Identity Theft Tax Refund Fraud

File tax returns early.

- Provides less time for a fraudster to file in an individual's name.

- Consumers who experience identity theft tax refund fraud can file affidavits with the Internal Revenue Service (IRS) and through IdentityTheft.gov, and may be eligible to obtain an Identity Protection Personal Identification Number from IRS.



Government Benefits Fraud

Set up an online account at the Social Security Administration and check it regularly.

- Can spot suspicious activity, such as benefits redirected to another address.

- Other government benefits, such as unemployment insurance, also can be susceptible to identity fraud.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

How to Respond after Identity Theft



Consumer Option

How This Option Can Help

Consumers Should Be Aware



Visit [identityTheft.gov](https://www.identitytheft.gov) to set up an account, fill out, and file necessary reports.

- Helps users determine what steps to take depending on the type of information stolen or type of identity theft.
- Can generate an Identity Theft Report that can be used to help contact consumer reporting agencies, law enforcement, and other entities.
- Can generate an IRS Identity Theft Affidavit (IRS Form 14039) that can be submitted directly to IRS.
- Provides information on what companies to contact and how to remove incorrect information.

- The Federal Trade Commission (FTC) also has a telephone help line and online chat feature.



Contact state or local government resources, such as consumer protection help lines or victim services offices.

- Some states and local governments can provide one-on-one assistance.

- States and localities vary in the services offered.



Consider using commercial identity restoration services.

- Can reduce consumer time and effort in dealing with the effects of identity theft, such as by interacting with creditors on the consumer's behalf.

- Service levels can vary significantly among companies. Some provide hands-on assistance, while others largely provide information.
- May be included in a package of identity theft services, which may also include credit or identity monitoring or identity theft insurance. Paid services typically cost \$5–\$30 a month and free services may only be offered for 1-2 years.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

Protect Personal Information in Other Ways



Consumer Option

How This Option Can Help

Consumers Should Be Aware



Adopt Good Practices for Online Accounts

- Protect passwords and do not re-use them.
- Use two-factor authentication when offered (for example, entering a one-time code sent to a mobile phone when logging in to an online account).
- Choose strong passwords and consider using a software application that helps manage passwords.
- Do not click on links in emails or open attachments from unknown senders.
- Remember that public WiFi may not be secure.

- While personal security practices are important, consumers have limited control over how private entities secure their data.



Protect social media accounts by checking privacy settings, and consider limiting information shared.

- Restricts how much information is visible to strangers and their ability to misuse it.

- Privacy terms and conditions can change, so it is important to check settings periodically.



Do not provide personal information over the phone (or by email or text) unless you've initiated the call (or communication).

- Prevents identity thieves from obtaining information that can be used to commit fraud.

- Consumers can do online searches to verify identities of requesters, or check with experts, before giving out information.
- Consumers should not trust caller ID and should hang up on robocalls and report such calls to FTC at ftc.gov/complaint.



Shred documents and mail with Social Security numbers or other personal information.

- Prevents identity thieves from finding sensitive information in trash.

- Consumers can contact the U.S. Postal Service if they believe their mail is being stolen or misdirected.
- Consumers can opt out of receiving credit card and other offers in the mail at 1-888-5-OPT-OUT (1-888-567-8688) or www.optoutprescreen.com.

Appendix III: GAO Contacts and Staff Acknowledgements

GAO Contact

Anna Maria Ortiz, (202) 512-8678 or ortiza@gao.gov

Staff Acknowledgments

In addition to the contact named above, Kay Kuhlman (Assistant Director), Meghana Acharya, Carl Barden, Bethany Benitez, Catherine Gelb (Analyst in Charge), Danielle Koonce, Jill Lacey, Kathleen McQueeney, Barbara Roesmann, Jena Sinkfield, and Meg Tulloch made significant contributions to this report.

Appendix IV: Accessible Data

Data Table

Accessible Data for Figure 2: Enrollment in Identity Theft Services Offered by Office of Personnel Management, October 2015–September 2018

Date	New enrollments (in thousands)
Oct. 2015	211.908
Nov. 2015	886.337
Dec. 2015	915.667
Jan. 2016	236.372
Feb. 2016	93.476
Mar. 2016	50.77
Apr. 2016	29.719
May 2016	17.166
June 2016	16.726
July 2016	80.591
Aug. 2016	46.897
Sept. 2016	14.203
Oct. 2016	9.124
Nov. 2016	15.835
Dec. 2016	25.262
Jan. 2017	24.199
Feb. 2017	8.583
Mar. 2017	6.676
Apr. 2017	4.424
May 2017	3.272
June 2017	3.338
July 2017	2.472
Aug. 2017	2.019
Sept. 2017	4.564
Oct. 2017	3.123
Nov. 2017	2.039
Dec. 2017	1.419
Jan. 2018	1.721
Feb. 2018	1.328

Appendix IV: Accessible Data

Date	New enrollments (in thousands)
Mar. 2018	1.223
Apr. 2018	1.05
May 2018	0.92
June 2018	0.748
July 2018	0.784
Aug. 2018	0.671
Sept. 2018	0.716

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<https://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <https://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/fraudnet/fraudnet.htm>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548



Please Print on Recycled Paper.