



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

October 20, 2023

The Honorable Cathy McMorris Rodgers, Chair
The Honorable Frank Pallone, Jr., Ranking Member
Committee on Energy and Commerce
United States House of Representatives
Washington, D.C. 20515

Dear Chair Rodgers and Ranking Member Pallone:

On behalf of the Federal Trade Commission, I am forwarding for your review a Report To Congress entitled The FTC's Efforts in the Greater Fight Against Ransomware and Cyber-Related Attacks. The Commission submits this report as directed by the "Reporting Attacks from Nations Selected for Oversight and Monitoring Web Attacks and Ransomware from Enemies Act," also known as the RANSOMWARE Act.¹ Thank you for your interest in the work of the Commission.

By direction of the Commission.

A handwritten signature in blue ink, appearing to read "April J. Tabor".

April J. Tabor
Secretary

Enclosure

¹ Consolidated Appropriations Act, 2023, Division BB, Title V, Public Law No: 117-328, *available at* <https://www.congress.gov/bill/117th-congress/house-bill/2617/text>.



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

October 20, 2023

The Honorable Maria Cantwell, Chair
The Honorable Ted Cruz, Ranking Member
Committee on Commerce, Science and Transportation
United States Senate
Washington, D.C. 20510

Dear Chair Cantwell and Ranking Member Cruz:

On behalf of the Federal Trade Commission, I am forwarding for your review a Report To Congress entitled The FTC's Efforts in the Greater Fight Against Ransomware and Cyber-Related Attacks. The Commission submits this report as directed by the "Reporting Attacks from Nations Selected for Oversight and Monitoring Web Attacks and Ransomware from Enemies Act," also known as the RANSOMWARE Act.¹ Thank you for your interest in the work of the Commission.

By direction of the Commission.

A handwritten signature in blue ink, appearing to read "April J. Tabor".

April J. Tabor
Secretary

Enclosure

¹ Consolidated Appropriations Act, 2023, Division BB, Title V, Public Law No: 117-328, *available at* <https://www.congress.gov/bill/117th-congress/house-bill/2617/text>.

The FTC's Efforts in the Greater Fight Against Ransomware and Cyber-Related Attacks

A Report to Congress

October 20, 2023



FEDERAL TRADE COMMISSION

Lina M. Khan, Chair
Rebecca Kelly Slaughter, Commissioner
Alvaro M. Bedoya, Commissioner

Contents

- Executive Summaryi**
- I. The FTC’s Efforts in the Greater Fight Against Ransomware and Cyber-Related Attacks1**
 - A. The FTC’s Data Security Program 2
 - B. Tech Support Scams 7
 - C. Protecting Consumers and Businesses Through Public Education and Guidance 9
- II. Additional Enforcement Actions Involving China and Russia: Privacy, Data Security, and Fraud and Other Deception12**
 - A. Privacy and Data Security Enforcement Actions 13
 - B. Fraud and Other Deception Enforcement Actions 16
 - C. FTC Warning Letters to Chinese Companies 18
- III. Cross-Border Cooperation with China and Russia.....19**
- IV. Consumer Complaint Data and Trends Related to Ransomware, Tech Support Scams, and China, Russia, North Korea, and Iran22**
 - A. The Consumer Sentinel Network 24
 - B. Consumer Sentinel Complaints about Malware and Tech Support Scams 24
 - 1. Malware and Computer Exploits 25
 - 2. Tech Support Scams 26
 - C. Consumer Sentinel Complaints about China, Russia, North Korea, and Iran 28
 - 1. China..... 29
 - 2. Russia..... 30
 - 3. North Korea 31
 - 4. Iran 32
- V. Legislative and Business Recommendations32**
- Acknowledgments35**

Executive Summary

The FTC respectfully submits this report as directed by the “Reporting Attacks from Nations Selected for Oversight and Monitoring Web Attacks and Ransomware from Enemies Act,” also known as the RANSOMWARE Act.¹

The FTC plays an important role in protecting the public against ransomware and other cyber-related attacks, complementing the work of other U.S. government agencies in the greater fight against these threats.² The FTC pursues a robust data security enforcement program to ensure that companies take appropriate steps to protect the personal data they hold against ransomware and other cyber-related attacks; pursues bad actors involved in ransomware-related “tech support” scams and other cyber exploits; and educates the public and businesses on how to best protect themselves and their data from such attacks. In addition, the FTC collects consumer complaints that include data related to fraud, ransomware, and other cyber-related attacks—data that it shares with other enforcement agencies and that can sometimes help to identify the location of entities involved in these illicit activities. These reports help the FTC and other enforcers spot trends and prioritize enforcement activities.

This report addresses the FTC’s activities as to ransomware and cyber-related attacks, and as to the four countries³ identified by the RANSOMWARE Act (China, Russia, North Korea, and Iran), as follows:

¹ Consolidated Appropriations Act, 2023, Division BB, Title V, Public Law No: 117-328, *available at* <https://www.congress.gov/bill/117th-congress/house-bill/2617/text>. In Sections 503(a)(1), (2), (3), and (5) of the RANSOMWARE Act, Congress directed the FTC to transmit a report providing details on cross-border complaints and complaint trends related to incidents, ransomware, or other cyber-related attacks reported to the Commission as committed by individuals, governments, or companies, including those located within or with ties to the governments of Russia, China, North Korea, or Iran, and a description of any related FTC litigation brought in foreign courts. In Section 503(a)(4), Congress requested the FTC to identify and provide details of foreign agencies located in Russia, China, North Korea, or Iran with which the Commission has cooperated. Last, in Sections 503(a)(6) through (8), Congress sought recommendations for legislation that may assist the FTC in carrying out the U.S. SAFE WEB Act of 2006 or may advance the security of the United States or U.S. companies, and recommendations for U.S. businesses and citizens to implement best practices on mitigating such attacks. In addition, Congress requested in Section 503(a) additional reports in 2025 and 2027.

² U.S. law enforcement agencies leading the fight against ransomware include the Federal Bureau of Investigation (FBI); Department of Homeland Security, Cybersecurity & Infrastructure Security Agency (CISA); the U.S. Secret Service; and the U.S. Department of Justice, Criminal Division. *See, e.g.*, FBI, How We can Help You, Ransomware, <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware> (last accessed Sept. 26, 2023); CISA, Ransomware Threat to OT (Jun. 9, 2021), <https://www.cisa.gov/resources-tools/resources/ransomware-threat-ot>; CISA Factsheet, Rising Ransomware Threat to Operational Technology Assets, Reporting at 3, *available at* https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf; U.S. Secret Service, Preparing for a Cyber Incident, <https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident> (last accessed Sept. 26, 2023); U.S. Secret Service, Cybercrime Investigations, Preparing for a Cyber Incident, A Guide to Ransomware at 2, *available at* <https://www.secretservice.gov/sites/default/files/reports/2021-11/Preparing%20for%20a%20Cyber%20Incident%20-%20A%20Guide%20to%20Ransomware%20v%201.1.pdf>; Department of Justice, CCIPS, Cybersecurity Unit (Apr. 12, 2022), <https://www.justice.gov/criminal-ccips/cybersecurity-unit>.

³ The Act refers in particular to the Russian Federation, the People’s Republic of China, the Democratic People’s Republic of Korea, and the Islamic Republic of Iran. The report refers to these countries with the shorter names Russia, China, North Korea, and Iran.

- [Section I](#) summarizes FTC activities addressing ransomware and other cyber-related attacks. This includes enforcement against data security practices that leave consumers or their data vulnerable to ransomware and other cyber-related attacks. It also covers enforcement actions concerning tech support scams, which sometimes involve taking control of consumers' computers and then demanding a ransom payment. Complementing this enforcement work is FTC consumer and business education about how to spot and avoid such harms and the FTC's outreach to and cooperation with foreign partners.⁴
- [Section II](#) describes additional FTC enforcement actions involving China and Russia, including on privacy, data security, fraud and other deception, as well as warning letters to Chinese companies.
- [Section III](#) addresses cross-border cooperation on the subjects described in the report with government agencies in China and Russia.⁵
- [Section IV](#) provides consumer complaint data and trends related to ransomware and other cyber-related attacks, tech support scams, and individuals, companies or governments with ties to the four countries identified in the RANSOMWARE Act. The FTC provides further international complaint data in a companion report submitted at the same time to Congress: "The U.S. SAFE WEB Act and the FTC's Fight Against Cross-Border Fraud."⁶
- [Section V](#) offers legislative recommendations to advance the FTC's mission in carrying out the U.S. SAFE WEB Act,⁷ and to protect the security of the United States and U.S. companies against ransomware and other cyber-related attacks. The section also offers best practice recommendations for U.S. businesses and consumers dealing with such threats.

⁴ The FTC has not engaged in foreign litigation regarding the topics identified in the RANSOMWARE Act.

⁵ The FTC has not engaged in cooperation with North Korea or Iran.

⁶ See FTC, The U.S. SAFE WEB Act and the FTC's Fight Against Cross-Border Fraud (Oct. 20, 2023) ("FTC 2023 SAFE WEB Report") at Section I and Appendix A. FTC reports are available at <https://www.ftc.gov/policy/reports/commission-staff-reports>.

⁷ Pub. L. No. 109-455, 120 Stat. 3372 (2006) (codified in scattered sections of 15 U.S.C. and 12 U.S.C. § 3412(e)). Congress also requested recommendations for legislation that may assist the FTC in carrying out the SAFE WEB Act in its 2020 law extending the Act until 2027. Pub. L. No. 116-173, 134 Stat. 837 (2020), available at <https://www.congress.gov/116/plaws/publ173/PLAW-116publ173.pdf>.

I. The FTC's Efforts in the Greater Fight Against Ransomware and Cyber-Related Attacks

Ransomware is a type of cyber-related attack in which bad actors hold data or computer access hostage until payment.⁸ It is treated here as a subset of the broader category covered by the RANSOMWARE Act: cyber-related attacks. The FTC's civil law enforcement tools and actions play a significant role in the overall effort by U.S. agencies to protect consumers and businesses against ransomware and other cyber-related attacks. One of the agency's earliest matters involving something akin to ransomware took place in 2006: the Commission brought a federal lawsuit against operators of certain websites for downloading software that repeatedly disrupted consumers' computer use with a sequence of large pop-ups and music.⁹ The pop-ups alleged that consumers had signed up for a "free trial" that had expired and then demanded payment to make them go away.¹⁰ The FTC considered these as "extortionate tactics" analogous to holding a computer hostage unless a fee was paid.¹¹ The FTC secured a consent agreement that required removal of the software, barred future downloads, and mandated over \$500,000 in consumer redress.¹² Since then, ransomware and cyber-related attacks arise most often in FTC matters related to data security and tech support scams.

In other matters, the FTC has taken action against defendants manipulating software to engage in a variety of cyber-related exploits against consumers, from malware to "pagejacking" and "mousetrapping." For example, as long ago as 1999 the FTC targeted a "pagejacking" and "mousetrapping" scheme in which the perpetrators copied existing web pages and inserted coded instructions that redirected internet surfers to unrelated websites that contained sexually-explicit, adult-oriented material.¹³ Once there, consumers were "mouse trapped" by incapacitating their internet browser's "back" and "close" buttons, so that while they were trying to exit the perpetrators' site, they were sent to additional adult sites in an unavoidable, seemingly endless loop.¹⁴ Similarly, in 2005 the FTC charged a company and its principal with luring consumers to their website by offering free software, which was bundled with spyware that intercepted and replaced search results and barraged consumers' computers with pop-up ads, captured consumers' personal information, and transmitted the

⁸ See, e.g., FTC, Consumer Sentinel Network Subcategory Definitions, May 2023, PSC Description 53: Malware & Computer Exploits, available at https://www.ftc.gov/system/files/ftc_gov/pdf/CSNPSCFullDescriptions.pdf?utm_source=govdelivery (last accessed Oct. 5, 2023) ("[R]ansomware, a specially designed variant of malware that holds data hostage pending payment."); Press Release, FTC, FTC Offers Advice on How to Avoid and Respond to Ransomware Attacks (Nov. 10, 2016), <https://www.ftc.gov/news-events/news/press-releases/2016/11/ftc-offers-advice-how-avoid-respond-ransomware-attacks> ("Ransomware – malicious software that denies access to computer files until the victim pays a ransom").

⁹ See generally Press Release, FTC, Movieland Defendants Settle FTC Charges (Sept. 13, 2007), <https://www.ftc.gov/news-events/news/press-releases/2007/09/movieland-defendants-settle-ftc-charges>.

¹⁰ See *id.*

¹¹ See, e.g., *FTC v. Digital Enterprises, Inc. d/b/a Movieland.com, et al.*, No. CV06-4923 (C.D. Cal. Aug. 8, 2006), First Am. Compl., ¶¶ 23, 53-55, available at <https://www.ftc.gov/sites/default/files/documents/cases/2006/08/060808movielandcmplt.pdf>.

¹² See Press Release, FTC, Movieland Defendants Settle FTC Charges (Sept. 13, 2006), <https://www.ftc.gov/news-events/news/press-releases/2007/09/movieland-defendants-settle-ftc-charges>. Restoring the FTC's authority to provide redress to victims is one the recommendations discussed near the end of this Report.

¹³ See Press Release, FTC, FTC Halts Internet Highjacking Scam (Sept. 22, 1999), <https://www.ftc.gov/news-events/news/press-releases/1999/09/ftc-halts-internet-highjacking-scam>.

¹⁴ See *id.*

information to the defendants' servers.¹⁵ In a 2009 related action, a U.S. district court held the defendants in contempt for violating the settlement order from the 2005 case by engaging in further "phishing," "pagejacking," and "mousetrapping" scams.¹⁶ More recently, in 2019 and 2021 the FTC took actions against developers of stalkerware apps that allegedly allowed purchasers of the apps to monitor the mobile devices on which they were installed, without the knowledge or permission of the device's user, exposing sensitive information about device users, including the user's physical movements, online activities, photos, text messages, web histories, GPS locations, and other personal information.¹⁷

More notable is the FTC's longstanding enforcement program on data security, which focuses on businesses holding data—sometimes enormous amounts of the public's personal data—that can be subject to ransomware and other cyber-related attacks. Strong data security serves as a frontline defense against cyber attacks. While the goal of some ransomware attacks is to make a company's data unusable so the company is motivated to pay a ransom in order to return to business, many ransomware attacks exfiltrate consumer data collected by the company and threaten disclosure of that data unless the ransom is paid. Ransomware attackers thus often seek to capture these vast stores of personal information. The FTC has a robust data security program that seeks to ensure that businesses engage in reasonable practices to protect the data of their customers. Data breaches often result from businesses' faulty data security practices, and virtually always involve a cyber attack, often by individuals or entities that are difficult even for criminal law enforcers to track down.

In addition to prioritizing proactive defenses to cyber-related attacks through our data security efforts, the FTC has also responded to tech support scams. Tech support scammers want their victims to believe that they have a serious problem with their computer, like a virus. The scammers connect with people through computer pop-up warnings, phone calls, or online ads or websites in search results for tech support help. The scammers then trick people into paying for tech support services they do not need or to fix a problem that does not exist. The scammers often ask for payments by wiring money, putting money on a gift card, prepaid card, or cash reload card, or using cryptocurrency or a money transfer app because they know those types of payments can be hard to reverse.¹⁸ Finally, the FTC aims to protect the public and businesses from the risks posed by ransomware and cyber-attacks through a wide range of public guidance and education efforts.

A. The FTC's Data Security Program

Starting in 2002, the FTC undertook its first enforcement action against data security practices that put personal information at risk. Since then, data security has become a crucial enforcement program that has furthered protections for consumers and encouraged companies to prioritize safeguarding consumer

¹⁵ See Press Release, FTC, Court Orders Internet Pagejackers to Return Ill-Gotten Gains (Jul. 30, 2009), <https://www.ftc.gov/news-events/news/press-releases/2009/07/court-orders-internet-pagejackers-return-ill-gotten-gains>.

¹⁶ See *id.*

¹⁷ See Press Release, FTC, FTC Finalizes Order Banning Stalkerware Provider from Spyware Business (Dec. 21, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/12/ftc-finalizes-order-banning-stalkerware-provider-spyware-business>; Press Release, FTC, FTC Brings First Case Against Developers of "Stalking" Apps (Oct. 22, 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/10/ftc-brings-first-case-against-developers-stalking-apps>.

¹⁸ See FTC Consumer Advice, How to Spot, Avoid and Report Tech Support Scams, <https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams#Spotting> (last accessed Sept. 26, 2023).

data. To date, the FTC has brought more than 80 enforcement actions involving data security. These actions have involved security that did not match the company's promises, which the FTC challenges as deceptive under Section 5 of the FTC Act, 15 U.S.C. § 45. In some actions, the FTC has also alleged that companies' failure to implement reasonable security practices was unfair under Section 5 because, among other things, it caused or was likely to cause substantial consumer injury. In many of these cases, although not all, the Commission alleged that the company's failure to secure consumer data or the company's products and services resulted in some sort of breach, hack, or other attack. In addition to enforcing Section 5, the FTC has alleged violations of other laws as appropriate.

On the occasion of the FTC's 50th data security settlement in 2014, the Commission explained that its standard on data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities.¹⁹ The FTC does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the fact that a data security breach occurred does not mean that a company violated the law.²⁰ This standard is the touchstone of the FTC's data security work involving data breaches, which, as mentioned above, very often involve a third-party cyber-related attack. The FTC's 2021 report to Congress on Privacy and Security provides some examples of enforcement in this area.²¹

Faulty data security practices can also include a lack of training on how to handle spam. In 2007, the FTC held a Spam Summit noting that "spam had increasingly become a significant global vector for the dissemination of malware and the propagation of financial crimes."²² More recent FTC guidance focuses on recognizing and avoiding particular types of phishing that can exploit current concerns such as government relief, package delivery, and tax refunds.²³ These phishing activities can lead to identity theft and cyber attacks, such as ransomware. The FTC has warned that phishing emails make up most ransomware attacks.²⁴ Moreover, the scale and scope of data collection has made companies and consumers "sitting ducks" for malicious actors.²⁵ Therefore, adequate data security practices should involve not only taking reasonable steps to safeguard data, but also limiting the amount of data one

¹⁹ See FTC, Commission Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), *available at* <https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf>.

²⁰ *Id.*

²¹ See FTC Report to Congress on Privacy and Security (Sept. 13, 2021) at 3-5, *available at* https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf.

²² See Press Release, FTC, FTC Issues Staff Report on Malicious Spam and Phishing (Dec. 28, 2007), <https://www.ftc.gov/news-events/news/press-releases/2007/12/ftc-issues-staff-report-malicious-spam-phishing>.

²³ See FTC Consumer Advice, Tag: Phishing Scams, <https://consumer.ftc.gov/all-scams/phishing-scams> (last accessed Oct. 2, 2023).

²⁴ See FTC Business Guidance, Ransomware, <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/ransomware> (last accessed Oct. 2, 2023).

²⁵ See FTC, Statement of Commissioner Rohit Chopra Joined By Commissioner Rebecca Kelly Slaughter, Regarding Data Security and the Safeguards Rule, Commission File No. P145407 (Mar. 2, 2020) at 3, *available at* https://www.ftc.gov/system/files/documents/public_statements/1567795/final_statement_of_rchopra_re_safeguards.pdf.

company can collect and compile, the types of data one company can combine, and the ways in which data can be used and monetized.²⁶

Furthermore, engaging in ransomware or some other cyber-related attack typically constitutes a criminal offense, and thus many U.S. criminal enforcement agencies play a key role working on these challenges.²⁷ For instance, the FBI describes itself as “the lead federal agency for investigating cyber attacks and intrusions . . . working to unmask those committing malicious cyber activities, wherever they are.”²⁸ And the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) states that it serves as “the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience” and coordinates with many other agencies on combatting ransomware.²⁹

As a civil law enforcement agency, the Commission cannot bring criminal charges against the malicious actors involved in cyber-related attacks, and lacks authority to issue search and arrest warrants against bad actors, all of which are potent tools in the fight against cyber-related attacks. Instead, the FTC’s data security efforts center on company practices and their effects on protecting consumers’ information. The FTC pursues these efforts regardless of the identity, location, and origin of the underlying malicious actor, as such threats can come from almost anywhere in the world. The FTC also works in appropriate cases with federal agencies with criminal jurisdiction, including on issues involving ransomware and cyber related attacks, by sharing evidence, providing access to complaint data, and coordinating through our Criminal Liaison Unit.³⁰

As set forth in detail in the FTC’s companion report on the U.S. SAFE WEB Act, the FTC has a robust system to collect, analyze, and report about consumer fraud complaints.³¹ The FTC also supports the

²⁶ See *id.*; FTC, Start With Security, A Guide for Business (Jun. 2015), available at <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>; FTC, Start with Security: A Guide for Business, <https://www.ftc.gov/business-guidance/resources/start-security-guide-business> (last accessed Oct. 2, 2023).

²⁷ See, e.g., Press Release, FBI, FBI, Partners Dismantle Qakbot Infrastructure in Multinational Cyber Takedown (Aug. 29, 2023), <https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown> (reporting international “disruption of a botnet infrastructure used by cybercriminals to commit ransomware”); Press Release, Department of Justice, United States and EU Foster Cooperation Against Ransomware Attacks (Jun. 16, 2022), <https://www.justice.gov/opa/pr/united-states-and-eu-foster-cooperation-against-ransomware-attacks> (mentioning the participation of the Department of Justice’s Criminal Division, the FBI, the U.S. Secret Service, and the U.S. Homeland Security Investigations in “a series of presentations and panel discussions on topics such as transnational cooperation on ransomware investigations, victim remediation, and prosecution of criminal organizations.”); Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), <https://www.justice.gov/criminal-ccips> (last accessed Sept. 26, 2023) (CCIPS seeks “to deter and disrupt computer and intellectual property crime by bringing and supporting key investigations and prosecutions . . .”); Department of Justice, CCIPS, Cybersecurity Unit (Apr. 12, 2022), <https://www.justice.gov/criminal-ccips/cybersecurity-unit> (the Cybersecurity Unit works “to ensure that law enforcement authorities are used effectively to bring perpetrators to justice” and “to protect . . . individual victims from cyber attacks.”).

²⁸ FBI, What We Investigate: Cyber Crime, <https://www.fbi.gov/investigate/cyber> (last accessed Sept. 23, 2023).

²⁹ See Cybersecurity and Infrastructure Security Agency: About CISA, <https://www.cisa.gov/about> (last accessed Sept. 26, 2023); CISA, Stop Ransomware, General Information, <https://www.cisa.gov/stopransomware/general-information> (last accessed Sept. 26, 2023) (stating that additional federal agencies involved in the fight against ransomware and cyber attacks include the U.S. Secret Service and the National Institute of Standards and Technologies.)

³⁰ See generally FTC, Criminal Liaison Unit, <https://www.ftc.gov/enforcement/criminal-liaison-unit> (last accessed Sept. 26, 2023).

³¹ See, e.g., Section I and Appendices A and B of the FTC 2023 SAFE WEB Report; FTC, Consumer Sentinel Network, www.sentinel.gov (last accessed Sept. 29, 2023).

criminal investigation and prosecution of identity theft by serving as the federal clearinghouse for identity theft reports, part of the FTC's Consumer Sentinel Network database. The genesis of FTC investigations and cases on data security, however, is rarely consumer complaints. One reason for this is that consumers are typically unaware of how a particular data breach or compromise of their personal data has occurred. And, as explained further below, *see infra* [Section IV](#), consumers often do not file complaints, especially with the government. Instead, the FTC often learns about data breaches and may begin corresponding investigations into related company practices from sources *other than* consumer complaints, such as the media or from the companies themselves.³² Consumer complaints, nonetheless, may be useful to inform the FTC about the impact of a particular data breach on consumers, or as evidence to support the agency's enforcement allegations.

The Commission has taken enforcement action against data security practices that do not meet the aforementioned standard. For example, in the 2022 *CafePress* litigation,³³ an individual hacked into the company's network from outside the United States in 2019 and repeatedly stole consumer information, some of which was used in extortion attempts on consumers.³⁴ In an administrative complaint, the FTC alleged that CafePress failed to implement reasonable security measures to protect sensitive information stored on its network, including plain text Social Security numbers, inadequately encrypted passwords, and answers to password reset questions; the FTC alleged that the company also concealed multiple breaches from consumers.³⁵ Following a consent agreement, the Commission issued an order that requires the company to bolster its data security and requires its former owner to pay a half million dollars to compensate small businesses.³⁶ As a civil law enforcement agency, the focus of the FTC's investigation and legal action was the company's failures to provide security for the sensitive information it maintained rather than the malicious actor involved in criminal activity.

The Commission sometimes obtains information about the source of hacks involved in its data security cases. The agency is also aware of public reports that large Chinese companies often have ties to the Chinese Communist party.³⁷ Moreover, in some matters the Commission has received information

³² Companies occasionally inform us of their data breaches voluntarily and sometimes they are legally required to do so, such as under the Health Breach Notification Rule. *See* 16 CFR Part 318, *available at* <https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule>. The FTC is currently considering amendments to the Safeguards Rule to require financial institutions to report certain data breaches and other security events to the Commission. *See* 16 CFR part 314, *available at* <https://www.federalregister.gov/documents/2021/12/09/2021-25064/standards-for-safeguarding-customer-information>.

³³ *See* FTC, *CafePress*, In the Matter of (Jun. 24, 2022), <https://www.ftc.gov/legal-library/browse/cases-proceedings/1923209-cafepress-matter>.

³⁴ Press Release, FTC, FTC Takes Action Against CafePress for Data Breach Cover Up (Mar. 15, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover>.

³⁵ *See id.*

³⁶ *See In the Matter of [CafePress]*, Fed. Trade Comm'n No. C-4768, Decision and Order, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/192%203209%20-%20CafePress%20combined%20package%20without%20signatures.pdf.

³⁷ *See, e.g.*, Kenji Kawase, Nikkei Asia, China's companies rewrite rules to declare Communist Party ties (Oct. 31, 2022), <https://asia.nikkei.com/Business/Companies/China-s-companies-rewrite-rules-to-declare-Communist-Party-ties> ("[M]ore than two-thirds of the mainland-listed companies whose shares can be traded by international investors in Hong Kong -- 1,029 of 1,526 companies -- have articles of association that formalize the role of in-house Communist Party cells. Most have been rewritten during the Xi era."); *see also* Code of Corporate Governance, Art. 5, China Securities Regulatory Commission (2018), *available at* http://www.csrc.gov.cn/csrc_en/c102034/c1372459/1372459/files/P020190415336431477120.pdf (requiring publicly listed companies in China to set up "[o]rganizations of the Communist Party of China . . . to conduct the Party's activities" and to "provide necessary conditions for the activities of the Party organizations.").

suggesting that malicious actors involved in data breaches were located in China or Russia. For example, in *Equifax Inc.*, the FTC, the Consumer Financial Protection Bureau (CFPB), and 50 U.S. states and territories alleged in 2019 that the credit reporting company failed to take reasonable steps to secure its network, which led to a data breach in 2017 that affected approximately 147 million people.³⁸ Specifically, the FTC claimed that Equifax failed to patch its network after being alerted in early 2017 to a critical security vulnerability, leading to the breach that exposed millions of names and dates of birth, Social Security numbers, physical addresses, and other personal information that could lead to identity theft and fraud.³⁹ The company subsequently agreed to implement a comprehensive information security program and pay at least \$575 million as part of a global settlement.⁴⁰ Here too, the focus of the FTC's investigation and legal action was the company's practices rather than the malicious actors involved. In 2020, the DOJ indicted four members of China's military for this hack of Equifax,⁴¹ and the Director of National Intelligence attributed the hack to the government of China or cyber actors based in China.⁴²

Similarly, in *Ascension*, the server of the company's service provider was accessed roughly 52 times by unauthorized IP addresses, including from China and Russia.⁴³ In that case, the FTC in 2020 alleged that the company violated the Gramm-Leach Bliley Act's Safeguards Rule by failing to develop, implement, and maintain a comprehensive information security program and ensure third-party vendors are capable of implementing and maintaining appropriate safeguards for customer information.⁴⁴ The FTC alleged that a vendor that Ascension hired to perform text recognition scanning on mortgage documents stored the contents of the documents, including names, dates of birth, Social Security numbers, on a cloud-based server in plain text, without any protections to block unauthorized access.⁴⁵ As part of a settlement, the company agreed to bolster its data security protections and oversight of its vendors to ensure third-party providers are also complying with those safeguards.⁴⁶

While ransomware and cyber-related attacks typically involve acts and actors that criminal law enforcement agencies are primarily equipped to confront, the FTC's data security program serves as a first line of defense against those attacks. Through these data security efforts, the FTC addresses

³⁸ See Press Release, FTC, Equifax to Pay \$575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (Jul. 22, 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach>.

³⁹ See *id.*

⁴⁰ See *id.*; Press Release, FTC, FTC Encourages Consumers to Opt for Free Credit Monitoring, as part of Equifax Settlement (Jul. 31, 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-encourages-consumers-opt-free-credit-monitoring-part-equifax-settlement>.

⁴¹ See Press Release, U.S. Department of Justice, Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax, Remarks as Prepared for Delivery (February 10, 2020), <https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military>.

⁴² See The National Counterintelligence and Security Center, China's Collection of Genomic and Other Healthcare Data From America: Risks to Privacy and U.S. Economic and National Security (Feb. 2021) at 4, available at https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf.

⁴³ See *In the Matter of Ascension Data and Analytics, LLC*, Fed. Trade Comm'n 1923126, Compl., ¶ 11, available at <https://www.ftc.gov/system/files/documents/cases/1923126ascensioncomplaint.pdf>.

⁴⁴ See Press Release, FTC, FTC Finalizes Order with Mortgage Analytics Firm, Requiring it to Strengthen Security Safeguards, Increase Oversight of Vendors (Dec. 22, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/12/ftc-finalizes-order-mortgage-analytics-firm-requiring-it-strengthen-security-safeguards-increase>.

⁴⁵ See *id.*

⁴⁶ See *id.*

inadequate data security practices and requires companies to better protect consumer data. The FTC's data security work also addresses the risks to a wide variety of consumer data, such as Social Security numbers, health data, data about children, credit card information, bank account information, usernames, and passwords, in a broad range of sectors and platforms, including retail, financial, mobile, and social media.⁴⁷ Data security is of critical and growing importance to consumers, and the Commission will continue to ensure that companies employ reasonable measures to safeguard consumer data.⁴⁸

B. Tech Support Scams

The Commission also plays an important role in the fight against activities akin to ransomware by shutting down “tech support” scams. Tech support scams are a perennial form of imposter scams where fraudulent telemarketers pretend to be from a well-known tech company, such as Microsoft or McAfee, and convince consumers that there are problems with their computers. The fraudsters will often cold-call consumers, using spoofed caller ID information, or use pop-up ads or messages warning consumers of a serious computer problem and directing them to call “tech support.” The scammers then employ a litany of tactics, including asking consumers for remote access to their computers in order to access information, enrolling consumers in worthless maintenance or warranty programs, and obtaining credit card information to bill consumers for worthless services. In some instances, the fraudsters will misrepresent that the consumers' computers have already been infected with malicious software (or “malware”), such as a virus or spyware,⁴⁹ or install malware that gives them access to sensitive data.

The FTC has taken action against perpetrators of tech support fraud, including by cooperating with foreign counterparts to stop scammers harming U.S. consumers from abroad.⁵⁰ In 2012, in *Pecon Software* and related matters,⁵¹ the FTC launched a major international crackdown of tech support scams, bringing six legal actions against a total of 14 corporate defendants and 17 individual defendants.⁵² The operations, based in India and targeting English-speaking consumers in the United States and other countries, including Canada, Australia, Ireland, New Zealand, and the United Kingdom, masqueraded as major computer companies and conned consumers into believing that their computers were riddled with viruses, spyware, and other malware, and then charged them fees ranging from \$49 to

⁴⁷ See FTC, Commission Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), available at <https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf>.

⁴⁸ See *id.*

⁴⁹ See FTC, Combatting Spyware and Malware, <https://www.ftc.gov/news-events/topics/identity-theft/spyware-malware> (last accessed Sept. 26, 2023).

⁵⁰ Since 2012, the FTC has initiated law enforcement actions against at least 116 defendants associated with tech support scams.

⁵¹ See *FTC v. Pecon Software Ltd.*, No. 12-cv-7186 (S.D. NY., Sept. 24, 2012), available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/1123118-pecon-software-ltd-et-al>; *FTC v. Lakshmi Infosoul Services Pvt Ltd.*, 12-cv-191 (S.D. NY, Sept., 24, 2012), available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/1223245-lakshmi-infosoul-services-pvt-ltd>; *FTC v. Finmaestros, LLC*, No. 12-cv-7195 (S.D. NY, Sept. 24, 2012), available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/1223247-finmaestros-llc-et-al>; *FTC v. PCCare247 Inc.*, No. 12-cv-7189 (S.D. NY, Sept. 24, 2012), available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/122-3243-x120057-pccare247-inc-et-al>; *FTC v. Mikael Marczak, aka Michael Marczak, also dba Virtual PC Solutions*, no. 12-cv-7192 (S.D. NY, Sept. 24, 2012), available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/1223246-virtual-pc-solutions-mikael-marczak-aka-michael-marczak-et-al>; *FTC v. Zeal IT Solutions Pvt Ltd.*, No. 12-cv-7188 (S.D. NY, Sept. 24, 2012), available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/1223244-zeal-it-solutions-pvt-ltd-et-al>.

⁵² See Press Release, FTC, FTC Halts Massive Tech Support Scams (Oct. 3, 2012), <https://www.ftc.gov/news-events/news/press-releases/2012/10/ftc-halts-massive-tech-support-scams>.

\$450 to remotely access and “fix” the consumers’ computers. Five of the operations used telemarketing boiler rooms to call consumers; the sixth lured consumers through Google ads that appeared when consumers searched for their computer company’s tech support telephone number. The FTC cooperated in this crackdown with the Australian Communications and Media Authority (“ACMA”), the Canadian Radio-television and Telecommunications Commission (“CRTC”), and the U.K.’s Serious Organised Crime Agency.⁵³ Ultimately, a U.S. district court permanently banned the defendants from marketing any computer security-related technical support service and ordered them to pay more than \$5.1 million.⁵⁴ The CRTC and ACMA also brought administrative actions for violations of their Do Not Call laws.⁵⁵

The FTC engaged in a similar campaign in “Operation Tech Trap”—a nationwide and international crackdown on tech support scams.⁵⁶ As part of this coordinated effort, the FTC, along with other federal, state, and international partners, brought 29 law enforcement actions against tech support scams. Most of the scammers followed a similar pattern of misconduct where they caused consumers’ computers to display advertisements designed to resemble pop-up security alerts from Microsoft, Apple, or other technology companies. These ads warned consumers that their computers were infected with viruses, were being hacked, or were otherwise compromised, and urged them to call a toll-free number for assistance. Consumers who called the number were connected to a call center, told that the telemarketers needed remote access to their computer, and then subjected to high-pressure tactics where many were persuaded to pay hundreds of dollars for unnecessary computer repair services, service plans, anti-virus protection, or other products and services. Included within this suite of actions was the FTC’s lawsuit against *Help Desk National*,⁵⁷ where Canadian defendants allegedly worked to sell their sham services to U.S. consumers; other agencies pursued federal criminal charges against tech support scams. In addition, as part of this global effort, law enforcement in India brought two criminal law enforcement actions, one of which was aided by the German Police, resulting in the arrest of tech support scammers.⁵⁸

The FTC has also worked with government officials, law enforcement, private companies, and trade associations in India to combat this problem at the source.⁵⁹ These efforts included sponsoring a

⁵³ See *id.* The FTC also worked with Microsoft (a Sentinel data contributor) and other computer companies.

⁵⁴ See Press Release, FTC, Federal Court Orders Tech Support Scammers to Pay More Than \$5.1 Million (July 24, 2014), <https://www.ftc.gov/news-events/news/press-releases/2014/07/federal-court-orders-tech-support-scammers-pay-more-51-million>.

⁵⁵ See Press Release, FTC, FTC Halts Massive Tech Support Scams (Oct. 3, 2012), <https://www.ftc.gov/news-events/news/press-releases/2012/10/ftc-halts-massive-tech-support-scams>.

⁵⁶ See Press Release, FTC, FTC and Federal, State and International Partners Announce Major Crackdown on Tech Support Scams (May 12, 2017), <https://www.ftc.gov/news-events/news/press-releases/2017/05/ftc-federal-state-international-partners-announce-major-crackdown-tech-support-scams>; FTC, Operation Tech Trap, Law Enforcement Actions, https://www.ftc.gov/es/system/files/attachments/press-releases/la-ftc-y-otras-agencias-colegas-del-ambito-federal-estatal-e-internacional-anuncian-medidas-severas/operation_tech_trap_chart_of_actions.pdf (last accessed Sept. 28, 2023).

⁵⁷ See *FTC v. Big Dog Solutions LLC*, No. 16-cv-06607 (N.D. Ill., June 24, 2016), available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3042-x160045-help-desk-national>.

⁵⁸ See Shashank Shekar, DailyMail India, UP police arrests fraud Noida techies who duped customers in the US by offering fake technical support (Sep. 30, 2016, 7:14 pm), <https://www.dailymail.co.uk/indiahome/indianews/article-3816586/UP-police-arrests-fraud-Noida-techies-duped-customers-providing-fake-technical-support.html>.

⁵⁹ See Prepared Statement of the Federal Trade Commission Before the United States Senate Special Committee on Aging on Combatting Technical Support Scams (Oct. 21, 2015), available at https://www.ftc.gov/system/files/documents/public_statements/826561/151021techsupporttestimony.pdf.

roundtable in New Delhi to develop a long-term strategy for combatting various types of telemarketing fraud originating in India, including tech support scams. The roundtable brought together Indian and foreign law enforcement officials, as well as representatives from India's legitimate call center industry, technology companies, and consumer groups. The Canadian Radio-television and Telecommunications Commission and the United Kingdom's National Crime Agency also participated. The meeting ultimately led to the formation of a council of industry leaders and government officials dedicated to combatting Indian telemarketing fraud and the development of an action plan to address the problem. A follow-up conference in New Delhi focused on assisting Indian law enforcement to prosecute known telemarketing scammers operating in India. That conference concentrated on using banking data to identify scammers, improving processes for sharing information with Indian law enforcement about perpetrators of telemarketing scams, and developing methods to assist Indian law enforcement investigations. The FTC also has had discussions with India's telecommunications regulator—the Telecom Regulatory Authority of India—to explore options for preventing Indian telemarketing fraudsters from gaining access to the necessary infrastructure to place calls to American consumers. Moreover, the FTC works closely with foreign partners all over the globe on unsolicited marketing through the Unsolicited Communications Enforcement Network (UCENET).⁶⁰

These actions illustrate the important domestic and cross-border work the FTC has done to stop tech support scams and the harm they inflict on U.S. consumers.⁶¹ Moreover, the FTC has also worked to stop those who assist and facilitate such frauds. For example, in 2020 the FTC settled with the Canadian company *RevenueWire* and its CEO over allegations that they laundered credit card payments for, and assisted and facilitated, two tech support scams previously sued by the FTC.⁶² These settlements permanently banned the defendants from any further payment laundering, require them to thoroughly screen and monitor high-risk clients to ensure those clients are not misleading consumers, and required them to pay \$6.75 million.

C. Protecting Consumers and Businesses Through Public Education and Guidance

As the nation's leading consumer protection agency, the FTC works to alert and educate the public about ransomware, other cyber-related attacks, and tech support scams. The FTC provides guidance to consumers and businesses, including tools that they can use to protect themselves against such threats.

⁶⁰ See Press Release, FTC, FTC Joins FCC in Renewing Memorandum of Understanding to Promote Cross-Border Law Enforcement Efforts to Combat Spam, Scams, and Illegal Telemarketing (Sept. 21, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-joins-fcc-renewing-memorandum-understanding-promote-cross-border-law-enforcement-efforts-combat>.

⁶¹ Cf. *FTC v. Genius Technologies, LLC*, No. 3:18-cv-01096 (N.D. Cal., Feb. 21, 2018), available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/172-31110-x180025-genius-technologies-llc> (defendants alleged to have worked with Indian telemarketers to trick older Americans into buying bogus technical support services).

⁶² See *FTC v. RevenueWire, Inc.*, No. 1:20-cv-01032 (D.D.C., April 21, 2020), available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3087-revenuewire-inc>. In 2019, the FTC also reached a settlement with the multinational payment processing company *Nexway, Inc.* for allegedly serving as a facilitator for tech support scammers by engaging in credit card laundering. See *United States v. Nexway Sasu*, No. 1:23-cv-900 (D.D.C., April 3, 2023), available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/1923239-x230018-nexway-inc-matter>.

And the FTC has worked across government and beyond to raise awareness about these important issues.

The FTC, through public outreach, has informed and brought together key players on ransomware. In 2016, as part of a larger seminar series on emerging consumer technology issues, the FTC hosted a workshop focused on ransomware.⁶³ Recognizing that ransomware was one of the most challenging cybersecurity problems affecting consumers and businesses, this workshop brought together representatives from the FTC, academia, and private industry to discuss the threats caused by ransomware, defenses against it, and what to do if you are a victim of ransomware. In 2019, 2020, and 2021, the FTC also held Green Lights & Red Flags: FTC Rules of the Road for Business—free business workshops that covered a range of topics including data security.⁶⁴ More recently, in 2022, the FTC presented to approximately 300 attendees at the International Monetary Fund on cyber threats and how to avoid them. The FTC has also hosted webinars and other local events addressing data security basics for small businesses, such as identifying cyber risks, guarding against phishing attempts and ransomware, and developing a data breach response plan, including an event in 2023 hosted by the FTC's Southwest Regional Office.

The FTC's business education program on cybersecurity, including on ransomware, other cyber-related attacks, and tech support scams also focuses on small businesses that might not have legal or IT departments to help them navigate the world of cybersecurity. The FTC provides advice on protecting networks and data in plain, clear language that is easy to understand so that business owners can talk with their employees, vendors, and others about cybersecurity.⁶⁵ These materials include a central and easily accessible website that covers a range of cybersecurity topics such as ransomware (*see Photo 1*),⁶⁶ tech support scams,⁶⁷ and other cyber-related attacks, in both English and Spanish.⁶⁸ The FTC's business guidance efforts also include blog posts, podcasts, videos, and more. For example, the FTC has published blogs on ransomware prevention,⁶⁹ videos on defending against and responding to

⁶³ See FTC, Fall Technology Series: Ransomware, September 7, 2016, <https://www.ftc.gov/news-events/events/2016/09/fall-technology-series-ransomware> (last accessed Sept. 28, 2023).

⁶⁴ See generally Press Release, FTC, New Green Lights & Red Flags business seminar debuts in Atlanta (July 2, 2019), <https://www.ftc.gov/business-guidance/blog/2019/07/new-green-lights-red-flags-business-seminar-debuts-atlanta>; Press Release, FTC, Green Lights & Red Flags: FTC Rules of the Road for Business rocks on in Cleveland (Sept. 21, 2020), <https://www.ftc.gov/business-guidance/blog/2020/09/green-lights-red-flags-ftc-rules-road-business-rocks-cleveland>; Press Release, FTC, Green Lights & Red Flags: FTC Rules of the Road for Business (Jun. 24, 2021), <https://www.ftc.gov/news-events/events/2021/06/green-lights-red-flags-ftc-rules-road-business>.

⁶⁵ See FTC, Cybersecurity for small businesses, <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity> (last accessed Sept. 22, 2023).

⁶⁶ See FTC, Ransomware, <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/ransomware> (last accessed Sept. 22, 2023).

⁶⁷ See FTC, Tech Support Scams, <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/tech-support-scams> (last accessed Sept. 22, 2023).

⁶⁸ See FTC, Ciberseguridad para pequeños negocios, <https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad> (last accessed Sept. 29, 2023).

⁶⁹ See Leslie Fair, FTC, Ransomware risk: 2 preventive steps for your small business (Nov. 5, 2021), <https://www.ftc.gov/business-guidance/blog/2021/11/ransomware-risk-2-preventive-steps-your-small-business>; Ben Rosen, FTC, Ransomware prevention: An update for businesses (Dec. 11, 2020), <https://www.ftc.gov/business-guidance/blog/2020/12/ransomware-prevention-update-businesses>.

ransomware,⁷⁰ and even a quiz to test businesses' knowledge on ransomware.⁷¹ And in 2023, the FTC recorded a podcast on understanding cybersecurity and avoiding scams to address the needs of Native American small businesses. To reflect a wide range of expertise, the FTC has also cooperated with other key federal agencies, such as the National Institute of Standards and Technology, the Department of Homeland Security, and the Small Business Administration.⁷²



Photo 1 (FTC webpage providing resources for small business on cybersecurity, including ransomware)

The FTC's consumer education efforts include up-to-date alerts and advice about malware, cybersecurity, and tech support scams. The FTC has issued consumer alerts on cybersecurity,⁷³ protecting devices from cryptojacking,⁷⁴ malware from illegal video streaming apps,⁷⁵ what to do about email hacks,⁷⁶ and the use of ads for fake artificial intelligence to spread malicious software.⁷⁷ The FTC has published articles for consumers on recognizing, removing, avoiding, and protecting their computers

⁷⁰ See FTC, Defend Against Ransomware, <https://www.ftc.gov/media/71331> (last accessed Sept. 28, 2023); FTC, Ransomware - Cybersecurity for Small Business, <https://www.youtube.com/watch?v=cy2ZW49E2A> (last accessed Sept. 28, 2023).

⁷¹ See FTC, Ransomware Quiz, <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/quiz/ransomware> (last accessed Sept. 22, 2023).

⁷² As part of a wider U.S. Government effort to protect consumers and businesses from cyber threats, other federal agencies, such as the FBI, also provide guidance. See, e.g., FBI, How We Can Help You, On the Internet: Be Cautious When Connected, <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/on-the-internet> (last accessed Sept. 28, 2023); U.S. Secret Service, Preparing for a Cyber Incident, <https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident> (last accessed Sept. 28, 2023).

⁷³ See Alvaro Puig, FTC, Cybersecurity advice to protect your connected devices and accounts (Mar. 23, 2022), <https://consumer.ftc.gov/consumer-alerts/2022/03/cybersecurity-advice-protect-your-connected-devices-and-accounts>.

⁷⁴ See Jason Adler, FTC, Protecting your devices from cryptojacking (June 7, 2018), <https://consumer.ftc.gov/consumer-alerts/2018/06/protecting-your-devices-cryptojacking>.

⁷⁵ See Alvaro Puig, FTC, Malware from illegal video streaming apps: What to know (May 2, 2019), <https://consumer.ftc.gov/consumer-alerts/2019/05/malware-illegal-video-streaming-apps-what-know>.

⁷⁶ See FTC, Hacked Email: What to Do, <https://www.ftc.gov/media/video-0104-hacked-email-what-do> (last accessed Sept. 28, 2023).

⁷⁷ See Alvaro Puig, FTC, Ads for fake AI and other software spread malicious software (Apr. 13, 2023), <https://consumer.ftc.gov/consumer-alerts/2023/04/ads-fake-ai-and-other-software-spread-malicious-software>.

from malware.⁷⁸ Similarly, the FTC has issued consumer alerts and published articles and infographics addressing various tech support scam issues. These have included advice on how to spot, avoid, and report tech support scams (*see Photo 2*),⁷⁹ and counsel consumers to never pay when someone demands a gift card or wire transfer through a service like MoneyGram or Western Union.⁸⁰



Photo 2 (Infographic on how to spot a tech support scam)

II. Additional Enforcement Actions Involving China and Russia: Privacy, Data Security, and Fraud and Other Deception

Apart from matters involving ransomware and cyber-related attacks, the FTC has taken enforcement actions that involve instances of known or unverified connections to China and Russia. These connections may involve the location of the companies or company officials involved; the location of servers; the destination of improper disclosures of data or funds; the origin of unauthorized access of information; and records and addresses obtained during investigations. These links to China and Russia have occurred most often in enforcement actions concerning violations of consumer privacy and data

⁷⁸ See FTC, How To Recognize, Remove, and Avoid Malware (May 2021), <https://consumer.ftc.gov/articles/how-recognize-remove-avoid-malware>; FTC, Protecting Your Computer From Malware, <https://consumer.ftc.gov/media/79889> (last accessed Sept. 22, 2023).

⁷⁹ See FTC, How To Spot, Avoid, and Report Tech Support Scams (Sept. 2022), <https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams>. See also Traci Armani, FTC, How can you spot a tech support scam? (Sept. 3, 2020), <https://consumer.ftc.gov/consumer-alerts/2020/09/how-can-you-spot-tech-support-scams>; FTC, Infographic: How to Spot a Tech Support Scam (Mar. 2019), <https://consumer.ftc.gov/articles/0557-infographic-how-spot-tech-support-scams>; Jim Kreidler, FTC, Hang up on tech support calls (Apr. 10, 2020), <https://consumer.ftc.gov/consumer-alerts/2020/04/hang-tech-support-calls>; FTC, How To Avoid a Tech Support Scam, <https://consumer.ftc.gov/media/video-0181-how-avoid-tech-support-scams> (last accessed Sept. 26, 2023); FTC, Tech Support Imposter Scams, <https://consumer.ftc.gov/media/79958> (last accessed Sept. 26, 2023).

⁸⁰ See Cristina Miranda, FTC, No gift cards for tech support scammers (June 6, 2018), <https://consumer.ftc.gov/consumer-alerts/2018/06/no-gift-cards-tech-support-scammers>.

security as well as fraud and other deception. The FTC also has sent warning letters to Chinese companies that may have violated laws that the FTC enforces.

A. Privacy and Data Security Enforcement Actions

Regarding privacy and data security, the FTC takes enforcement action when companies deceive consumers that they will not share their information and then do so, or when companies share information in ways that consumers would not expect and cause substantial consumer injury. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair or deceptive acts or practices in or affecting commerce.⁸¹ In addition to the FTC Act, the FTC also enforces other federal laws relating to consumers' privacy and data security, such as the Children's Online Privacy Protection Act, Fair Credit Reporting Act, Gramm-Leach-Bliley Act, and Health Breach Notification Rule.⁸²

As mentioned above, some of the Commission's enforcement actions concerning privacy and data security involve connections to China. For example, in *Easy Healthcare*, a lawsuit filed in federal court by the DOJ on behalf of the FTC in 2023, the Commission charged that the developer of the fertility app Premom deceived users by sharing their sensitive personal information with third parties—including two China-based firms; disclosed users' sensitive health data to AppsFlyer and Google; and failed to notify consumers of these unauthorized disclosures.⁸³ The FTC alleged that the data that the company shared with third parties revealed highly sensitive and private details about Premom's users and led to the unauthorized disclosure of facts about an individual user's sexual and reproductive health, parental and pregnancy status, as well as other information about physical health conditions and status.⁸⁴ Moreover, according to the complaint, Premom did not limit third-parties' use of the data and failed to encrypt adequately the data that it shared with third parties, including those in China, subjecting it to potential interception or seizure.⁸⁵ Under a stipulated order, the company agreed to certain requirements, including not sharing user personal health data with third parties for advertising; obtaining user consent before sharing personal health data with third parties for other purposes; seeking deletion of data it shared with third parties; implementing comprehensive security and privacy programs; and paying a \$100,000 civil penalty for violating the Health Breach Notification Rule.⁸⁶

⁸¹ See 15 U.S.C. §45.

⁸² See generally FTC, Division of Privacy and Identity Protection, <https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity> (last accessed Sept. 22, 2023).

⁸³ See Press Release, FTC, Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order (May 17, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc>; see also *United States v. Easy Healthcare Corporation*, No. 23-cv-3107 (N.D. Ill. May 17, 2023), ECF No. 1: Compl., available at https://www.ftc.gov/system/files/ftc_gov/pdf/2023186easyhealthcarecomplaint.pdf. These acts violated the Health Breach Notification Rule and Section 5 of the FTC Act.

⁸⁴ See Press Release, FTC, Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order (May 17, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc>

⁸⁵ See *id.*

⁸⁶ See *id.*

In *Zoom*, the FTC in 2020 alleged that Zoom misled users by touting that it offered “end-to-end, 256-bit encryption” to secure users’ communications, when in fact it provided a lower level of security.⁸⁷ According to the allegations, Zoom’s servers—including some located in China—maintained the cryptographic keys that could allow Zoom to access the content of its customers’ meetings.⁸⁸ Zoom’s misleading claims also gave users a false sense of security, according to the FTC’s complaint, especially for those who used the company’s platform to discuss sensitive topics such as health and financial information.⁸⁹ Additional allegations included misleading some users by falsely claiming that meetings were encrypted immediately after the meeting ended; secretly installing software that automatically launched and joined a user to a meeting by bypassing a safeguard that protected users from a common type of malware; and not implementing any offsetting measures to protect users’ security and increasing users’ risk of remote video surveillance by strangers.⁹⁰ As part of a settlement, the company agreed to certain requirements, including establishing and implementing a comprehensive security program; a prohibition on privacy and security misrepresentations; reviewing any software updates for security flaws prior to release and ensuring the updates will not hamper third-party security features; and informing the FTC of any data breaches.⁹¹

Furthermore, in 2019 the Commission, represented by the DOJ, brought a lawsuit against the video social networking app *Musical.ly*, now known as TikTok, alleging that the company illegally collected personal information from children.⁹² According to the complaint, Musical.ly’s principal place of business was Shanghai, China, and the company had been previously acquired by ByteDance, Ltd. (also based in China)⁹³ and merged with the TikTok app under the TikTok name.⁹⁴ According to the FTC, the Musical.ly app required users to provide an email address, phone number, username, first and last name, a short biography, and a profile picture to create and share short videos, interact with other users, and send direct messages.⁹⁵ Further, the operators of Musical.ly knew many children were using the app and received complaints from parents, but they still failed to seek parental consent before collecting names,

⁸⁷ See Press Release, FTC, FTC Requires Zoom to Enhance its Security Practices as Part of Settlement (Nov. 9, 2020), <https://www.ftc.gov/news-events/news/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement>; see generally FTC, Zoom Video Communications, Inc., In the Matter of, <https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3167-zoom-video-communications-inc-matter> (last accessed Sept. 28, 2023).

⁸⁸ See *In the Matter of Zoom Video Communications, Inc.*, Fed. Trade Comm’n 192-3167, Compl. ¶ 24, <https://www.ftc.gov/system/files/documents/cases/1923167zoomcomplaint.pdf>.

⁸⁹ See Press Release, FTC, FTC Requires Zoom to Enhance its Security Practices as Part of Settlement (Nov. 9, 2020), <https://www.ftc.gov/news-events/news/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement>;

⁹⁰ See *id.*

⁹¹ See *id.*; Press Release, FTC, FTC Gives Final Approval to Settlement with Zoom over Allegations the Company Misled Consumers about Its Data Security Practices (Feb. 1, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/02/ftc-gives-final-approval-settlement-zoom-over-allegations-company-misled-consumers-about-its-data>.

⁹² Press Release, FTC, Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children’s Privacy Law (Feb. 27, 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc-allegations-it-violated-childrens-privacy>.

⁹³ See, e.g., Zheping Huang, TIME, ByteDance, TikTok’s Chinese Parent Company, Is Testing an AI Chatbot (Jun. 9, 2023 1:00 am), <https://time.com/6286069/bytedance-tiktok-artificial-intelligence-chatbot-china/> (referring to ByteDance as a “Chinese company”).

⁹⁴ *United States v. Musical.ly*, No. 19-cv-1439 (C.D. Cal. Feb. 27, 2019), ECF No. 1: Compl. ¶¶ 8, 23, available at https://www.ftc.gov/system/files/documents/cases/musical.ly_complaint_ecf_2-27-19.pdf

⁹⁵ Press Release, FTC, Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children’s Privacy Law (Feb. 27, 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc-allegations-it-violated-childrens-privacy>.

email addresses, and other personal information from users under the age of 13.⁹⁶ And user accounts were public by default, which meant that a child's profile bio, username, picture, and videos could be seen by other users, and there were public reports of adults trying to contact children via the Musical.ly app.⁹⁷ In addition to a \$5.7 million monetary payment, a settlement required the app's operators to comply with the Children's Online Privacy Protection Act going forward and to take offline all videos made by children under the age of 13.⁹⁸ Congress's Committee on Energy and Commerce recently held a hearing that expressed concerns about the scope of TikTok's data collection and data security practices."⁹⁹

In the 2018 *BLU* litigation, the FTC claimed that a mobile phone manufacturer and its co-owner allowed a China-based third-party service provider to collect detailed personal information about consumers, such as text message contents and real-time location information, without their knowledge or consent despite promises by the company that it would keep such information secure and private.¹⁰⁰ Specifically, according to the complaint, the company falsely claimed that they limited third-party collection of data from users of BLU's devices to only information needed to perform requested services and falsely represented that they had implemented "appropriate" physical, electronic, and managerial procedures to protect consumers' personal information.¹⁰¹ Instead, the China-based third-party service provider collected and transferred to its servers far more information than needed to do its job, including sensitive personal information and the full content of consumers' text messages, real-time location data, call and text message logs with full telephone numbers, contact lists, and lists of applications used and installed on BLU devices.¹⁰² And, as alleged in the FTC's complaint, BLU continued to allow the China-based third-party service provider to operate on its older devices without adequate oversight despite previously claiming that it had updated its software and had stopped its unexpected data collection practices.¹⁰³ A settlement with the FTC requires the defendants to not misrepresent the extent to which they protect the privacy and security of personal information; implement and maintain a comprehensive security program that addresses security risks associated with new and existing mobile devices and protects consumer information; and be subject to third-party assessments of the company's security program every two years for 20 years.¹⁰⁴

⁹⁶ *See id.*

⁹⁷ *See id.*

⁹⁸ *See id.*

⁹⁹ *See* U.S. House of Representatives, Energy and Commerce Committee, Chair Rodgers to TikTok CEO: "Your Platform Should be Banned" (May 23, 2023), <https://energycommerce.house.gov/posts/chair-rodgers-to-tik-tok-ceo-your-platform-should-be-banned>.

¹⁰⁰ Press Release, FTC, Mobile Phone Maker BLU Reaches Settlement with FTC over Deceptive Privacy and Data Security Claims (Apr. 30, 2018), <https://www.ftc.gov/news-events/news/press-releases/2018/04/mobile-phone-maker-blu-reaches-settlement-ftc-over-deceptive-privacy-data-security-claims>.

¹⁰¹ *See id.*

¹⁰² *See id.*

¹⁰³ *See id.*

¹⁰⁴ Press Release, FTC, FTC Gives Final Approval to Settlement with Phone Maker BLU (Sept. 10, 2018), <https://www.ftc.gov/news-events/news/press-releases/2018/09/ftc-gives-final-approval-settlement-phone-maker-blu>.

B. Fraud and Other Deception Enforcement Actions

The FTC targets scams and bad business practices that cheat people out of money.¹⁰⁵ The Commission provides consumers education resources and the ability to submit reports of suspected fraud, which it uses for investigations and shares with more than 2,800 law enforcers.¹⁰⁶ The most commonly reported types of fraud in 2022 were imposter scams; online shopping scams; prizes, sweepstakes, and lotteries; investment related reports; and business and job opportunities.¹⁰⁷

As outlined in the companion report on the U.S. SAFE Web Act, the FTC has also seen numerous complaints by consumers about Chinese companies. As noted below, between January 1, 2019, and June 30, 2023, consumers reported 89,450 complaints about business conduct originating in China. Here too, the Commission has encountered links to China in its enforcement work, as well as some indications of the potential involvement of actors from Russia.

For example, in the 2020 *Clorox Impostor* litigation consumers reported that websites claimed they could provide Clorox and Lysol products, but consumers never received the products after submitting their orders and payment information.¹⁰⁸ The investigation revealed the involvement of people outside the United States, including .ru extensions on emails (.ru is the country code top level domain for Russia, though its use may not necessarily entail operations within Russia),¹⁰⁹ records with information in Chinese,¹¹⁰ website registrant addresses in China,¹¹¹ and a PayPal account held in China.¹¹² According to the FTC's complaint, during the COVID-19 pandemic counterfeit websites were aimed at consumers urgently seeking cleaning and disinfecting products and were designed to look like genuine sellers offering Clorox and Lysol products.¹¹³ In some cases, consumers reported that when they tried to return to the fake website to seek a refund, it was gone in a matter of days or weeks, while the defendants moved on to set up a new website with a different URL.¹¹⁴ Where consumers sought

¹⁰⁵ See, e.g., FTC, Bureau of Consumer Protection, Fighting Scams and Fraud, <https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection> (Sept. 25, 2023); FTC, Impostor Scams, <https://www.ftc.gov/office-inspector-general/ftc-imposter-scams> (last accessed Oct. 2, 2023).

¹⁰⁶ See FTC, Report to Help Fight Fraud!, <https://reportfraud.ftc.gov/#/> (last accessed Sept. 26, 2023); see also FTC, Why Report Fraud?, <https://www.ftc.gov/media/why-report-fraud-0> (last accessed Sept. 26, 2023).

¹⁰⁷ Press Release, FTC, New FTC Data Show Consumers Reported Losing Nearly \$8.8 Billion to Scams in 2022 (Feb. 23, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022>.

¹⁰⁸ See Press Release, FTC, Court Issues Order Halting Operators of Fake Websites Claiming to Sell Clorox and Lysol Products (Nov. 5, 2020), <https://www.ftc.gov/news-events/news/press-releases/2020/11/court-issues-order-halting-operators-fake-websites-claiming-sell-clorox-lysol-products>; *FTC v. One or More Unknown Parties Deceiving Consumers Into Making Purchases Through: www.cleanyos.com, et al.*, No. 20-cv-02494 (N.D. Oh. Nov. 4, 2020), ECF No. 1: Compl. ¶¶ 8-20, available at https://www.ftc.gov/system/files/documents/cases/complaint_w-a_filed.pdf.

¹⁰⁹ See *FTC v. One or More Unknown Parties Deceiving Consumers Into Making Purchases Through: www.cleanyos.com, et al.*, No. 20-cv-02494 (N.D. Oh. Nov. 4, 2020), ECF No. 2-3: Decl. ¶ 23-vii.

¹¹⁰ See *id.*

¹¹¹ See *FTC v. One or More Unknown Parties Deceiving Consumers Into Making Purchases Through: www.cleanyos.com, et al.*, No. 20-cv-02494 (N.D. Oh. Nov. 11, 2020), ECF No. 9-1: Decl. ¶ 7-C-iii.

¹¹² See *id.* ¶ 13-d.

¹¹³ See Press Release, FTC, Court Issues Order Halting Operators of Fake Websites Claiming to Sell Clorox and Lysol Products (Nov. 5, 2020), <https://www.ftc.gov/news-events/news/press-releases/2020/11/court-issues-order-halting-operators-fake-websites-claiming-sell-clorox-lysol-products>.

¹¹⁴ See *id.*

chargebacks from their credit card companies, they found that the defendants used falsified shipment information to make it harder for consumers to get the charges reversed.¹¹⁵ The FTC obtained from a U.S. district court a temporary restraining order and a preliminary injunction, which effectively shut down approximately 100 fraudulent websites.¹¹⁶ The Commission asked the court for time to find and serve the defendants,¹¹⁷ but subsequently voluntarily dismissed the case without prejudice, noting that the aforementioned orders disrupted and effectively put an end to the scheme and that no defendant appeared.¹¹⁸

The 2017 *Western Union* litigation is another case with links to China and an example of the FTC's enforcement cooperation on matters that involve criminal activities.¹¹⁹ Western Union entered into agreements with the FTC, DOJ, and several U.S. Attorney's offices stemming from claims that the company's money services business facilitated fraud, scammers, and rip offs and resulted in the processing of hundreds of millions of dollars in prohibited transactions.¹²⁰ In this case, hundreds of millions of dollars were sent to China in structured transactions designed to avoid the reporting requirements of the Bank Secrecy Act, which the company knew about for at least five years.¹²¹ For example, a Western Union agent office in the United States sent over \$310 million to China in a span of five years, half of which was illegally structured and transmitted using false identification.¹²²

The FTC's complaint charged that for many years, fraudsters around the world used Western Union's money transfer system even though the company had long been aware of the problem, and that some Western Union agents had been complicit in fraud.¹²³ For example, agents often processed the fraud payments for the fraudsters in return for a cut of the fraud proceeds.¹²⁴ The FTC's complaint further alleged that Western Union declined to put in place effective anti-fraud policies and procedures and failed to act promptly against problem agents, identifying them but profiting from their actions by not promptly suspending and terminating them.¹²⁵ In resolving the FTC charges, Western Union agreed to a monetary judgment of \$586 million for refunds to consumers who were harmed by the company's unlawful behavior; implementation of a comprehensive anti-fraud program with training for its agents and their front line associates; monitoring to detect and prevent fraud-induced money transfers; due diligence on all new and renewing company agents; and suspension or termination of noncompliant agents.¹²⁶ Similarly, Western Union admitted its criminal violations to the criminal law enforcement

¹¹⁵ *See id.*

¹¹⁶ *FTC v. One or More Unknown Parties Deceiving Consumers Into Making Purchases Through: www.cleanyos.com, et al.*, No. 20-cv-02494 (N.D. Oh. Jan. 29, 2021), ECF No. 11: Pl's Status Report and Req. for Extension Pursuant to Rule 4(m).

¹¹⁷ *See id.*

¹¹⁸ *FTC v. One or More Unknown Parties Deceiving Consumers Into Making Purchases Through: www.cleanyos.com, et al.*, No. 20-cv-02494 (N.D. Oh. Jun. 8, 2022), ECF No. 13: Notice of Voluntary Dismissal Pursuant to Rule 41(a)(1)(A)(i).

¹¹⁹ *See generally* FTC, The Western Union Company (Sept. 23, 2020), <https://www.ftc.gov/legal-library/browse/cases-proceedings/122-3208-western-union-company>.

¹²⁰ Press Release, FTC, Western Union Admits Anti-Money Laundering Violations and Settles Consumer Fraud Charges, Forfeits \$586 Million in Settlement with FTC and Justice Department (Jan. 19, 2017), <https://www.ftc.gov/news-events/news/press-releases/2017/01/western-union-admits-anti-money-laundering-violations-settles-consumer-fraud-charges-forfeits-586>.

¹²¹ *See id.*

¹²² *See id.*

¹²³ *See id.*

¹²⁴ *See id.*

¹²⁵ *See id.*

¹²⁶ *See id.*

authorities, including willfully failing to maintain an effective anti-money laundering program and aiding and abetting wire fraud.¹²⁷ The company agreed to forfeit \$586 million and to enhanced compliance obligations to prevent a repeat of the charged conduct.¹²⁸ The DOJ noted its appreciation for the “significant cooperation and assistance” that the FTC provided in this matter.¹²⁹

Another category of cases involving China relates the FTC’s Made in America matters. As many firms look to onshore production and as many consumers look to buy “Made in America” goods, the FTC is taking comprehensive action to protect the integrity of the label and ensure a level playing field for domestic manufacturers. In 2021, the Commission finalized a rule that prohibits the misuse of the “Made in America” label, and the Commission has taken action to enforce this rule. In 2022, the FTC sued a U.S. apparel company, *Lions Not Sheep Products, LLC*, and its owner Sean Whalen for falsely claiming that its imported apparel was Made in USA.¹³⁰ According to the FTC’s complaint, the company added phony Made in USA labels to clothing and accessories imported from China and other countries.¹³¹ The FTC’s final order requires Lions Not Sheep and Whalen to stop making bogus Made in USA claims and pay a monetary judgment.¹³² The FTC’s enforcement work in this area includes other actions with false Made in USA claims involving goods actually made in China.¹³³

C. FTC Warning Letters to Chinese Companies

The FTC aims to eliminate false or misleading information from the marketplace.¹³⁴ For this purpose, the FTC sometimes sends letters, by itself or jointly with other enforcement agencies, to warn companies that their conduct is likely unlawful and that they can face legal consequences if they do not stop it.¹³⁵ Here too the Commission has encountered links to China in its enforcement work.

For example, in 2014 the FTC staff sent a letter to *BabyBus*, a China-based developer of mobile applications directed to children, warning that the company might be violating the Children’s Online Privacy Protection Act (COPPA) Rule by apparently collecting children’s location information without

¹²⁷ See *id.*

¹²⁸ See *id.*

¹²⁹ See *id.*

¹³⁰ Press Release, FTC, FTC Takes Action Against Lions Not Sheep and Owner for Slapping Bogus Made in USA Labels on Clothing Imported from China (May 11, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-takes-action-against-lions-not-sheep-owner-slapping-bogus-made-usa-labels-clothing-imported>.

¹³¹ See *id.*

¹³² See *id.*

¹³³ These matters include *Instant Brands*, see FTC, *Instant Brands LLC, In the Matter of* (Mar. 7, 2023), <https://www.ftc.gov/legal-library/browse/cases-proceedings/2223140-instant-brands-llc-matter> (allegedly falsely claiming that Pyrex-brand kitchen and home products, were made in the United States during a time some measuring cups were imported from China); *Electrowarmth Products*, see FTC, *Electrowarmth Products, LLC* (Oct. 28, 2022), <https://www.ftc.gov/legal-library/browse/cases-proceedings/222-3096-electrowarmth-products-llc> (allegedly false claims that heated fabric mattress pads were made in USA when in fact they were wholly imported from China); and *Gennex Media*, see FTC, *Gennex Media, In the Matter of* (Apr. 14, 2021), <https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3122-gennex-media-matter> (allegedly false claims that customizable promotional products such as wristbands, lanyards, temporary tattoos, and buttons were all or virtually all made in the United States when in numerous instances the products are wholly imported from China.).

¹³⁴ See FTC, *About FTC Warning Letters*, <https://www.ftc.gov/news-events/topics/truth-advertising/about-ftc-warning-letters> (last accessed Oct. 2, 2023).

¹³⁵ See *id.*

parental consent.¹³⁶ The letter asked the company to evaluate its apps and determine whether they may be in violation; informed the company that the Commission would review the apps again in the next month for compliance with the rule; and provided a copy of the letter to the Apple iTunes, Google Play Store, and Amazon Appstore.¹³⁷ For the same reasons, the Commission staff sent a warning letter in 2018 to China-based *Gator Group Co., Ltd.*, which advertised an app and device marketed as a “child’s first cell phone.”¹³⁸ More recently, in 2020, the FTC staff sent a warning letter to *Spooky2 Scalar*, a Chinese company, for unlawfully advertising that certain products treated or prevented Coronavirus Disease 2019 (COVID-19) without competent and reliable scientific evidence.¹³⁹ The letter advised the company to review its claims for such products and immediately cease making claims that were not supported by competent and reliable scientific evidence.¹⁴⁰

III. Cross-Border Cooperation with China and Russia

The FTC has had limited interactions with government agencies in the four countries covered by this report. In this section, as directed by Section 503(a)(4) of the RANSOMWARE Act, we identify the agencies with which we have interacted and the results of those interactions.¹⁴¹ As described below, the FTC and its staff have had limited interactions with government authorities in these countries, and to the best of our knowledge little or no direct enforcement cooperation on ransomware or cyber-related attacks.

FTC staff has had no interaction with agencies in either Iran or North Korea. U.S. consumers, as shown in the complaints analysis below, do not frequently report interactions with businesses in these countries. Moreover, the U.S. SAFE WEB Act provides that the FTC “may not provide investigative assistance [...] to a foreign law enforcement agency from a foreign state that the Secretary of State has determined

¹³⁶ See Press Release, FTC, FTC Warns Children’s App Maker BabyBus About Potential COPPA Violations (Dec. 12, 2014), <https://www.ftc.gov/news-events/news/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa-violations>; see generally FTC, Children’s Online Privacy Protection Rule (“COPPA”), <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa> (last accessed Oct. 2, 2023).

¹³⁷ See Press Release, FTC, FTC Warns Children’s App Maker BabyBus About Potential COPPA Violations (Dec. 12, 2014), <https://www.ftc.gov/news-events/news/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa-violations>; FTC Warning Letter to BabyBus (Fujian) Network Technology Co., Ltd. (Dec. 17, 2014), available at https://www.ftc.gov/system/files/documents/public_statements/606451/141222babybusletter.pdf.

¹³⁸ See Press Release, FTC, FTC Warns Gator Group, Tinitell that Online Services Might Violate COPPA (Apr. 27, 2018), <https://www.ftc.gov/news-events/news/press-releases/2018/04/ftc-warns-gator-group-tinitell-online-services-might-violate-coppa>.

¹³⁹ See FTC Warning Letter to Spooky2 Scalar Re: Unsubstantiated claims for Coronavirus prevention and treatment (May 4, 2020), available at https://www.ftc.gov/system/files/warning-letters/covid-19-letter_to_dap_spooky_2_scalar.pdf; see also Leslie Fair, FTC Business Blog, 50 more FTC warning letters say “Enough!” to questionable coronavirus claims (May 21, 2020), <https://www.ftc.gov/business-guidance/blog/2020/05/50-more-ftc-warning-letters-say-enough-questionable-coronavirus-claims>.

¹⁴⁰ See *id.*

¹⁴¹ Section 503(a)(4) of the RANSOMWARE Act directs the FTC to include in this report “[i]dentification and details of foreign agencies (including foreign law enforcement agencies . . . located in Russia, China, North Korea, or Iran with which the Commission has cooperated and the results of such cooperation, including any foreign agency enforcement action or lack thereof.”

[...] has repeatedly provided support for acts of international terrorism [...].”¹⁴² The Secretary of State has made that determination for Iran and North Korea during the time period covered by this report.¹⁴³

FTC staff has had limited interactions with agencies in Russia. Again, U.S. consumer complaints relating to Russia have been relatively few in number. FTC staff has participated in multilateral fora on consumer policy and privacy where Russian agencies have at times also participated.¹⁴⁴ The FTC has also interacted more directly with Russian authorities on technical assistance missions and related matters. Those contacts, however, date back to 2013 or earlier.

FTC staff has had more contact with agencies in China. This reflects in part the much larger number of consumer complaints about Chinese companies and the larger number of FTC cases that involve businesses connected in some way with China. It also reflects engagement on technical assistance and cooperation. Some of these contacts have focused on privacy and data security; others on scams and consumer protection.¹⁴⁵

The FTC engaged for many years with China’s former consumer protection authority, the State Administration for Industry and Commerce (SAIC), which in 2018 was reorganized into a larger agency called the State Administration for Market Regulation (SAMR). In 2007, the FTC and SAIC entered into a Memorandum of Understanding on Consumer Protection Matters.¹⁴⁶ This MOU provided for “exchanging views on consumer protection issues of common interest,” and “exploring the possibility of conducting mutual visits relating to important consumer protection issues that are of mutual concern.” The FTC then followed up with several missions to China to exchange information with SAIC officials; the FTC also hosted delegations from SAIC in Washington, D.C. These contacts focused on providing information about statutes enforced by the FTC in matters such as e-commerce, green claims, and multi-level marketing. FTC staff also participated in a Legislative Seminar at the invitation of the Government of China to discuss China’s then draft Electronic Commerce Law.

Notwithstanding the MOU and the FTC’s efforts at cooperation, SAIC declined as a general matter to provide assistance in resolving consumer complaints regarding Chinese online platforms and suppliers. FTC staff has since then raised the issue of cooperation with SAMR, SAIC’s successor, and looks forward to further discussion of this subject.

FTC staff did coordinate with the Chinese Embassy regarding scam calls directed at Chinese nationals across the United States. Callers posing as members of the Chinese government spoofed the numbers of the Chinese Embassy or Consulate and threatening Chinese nationals with arrest or deportation based on

¹⁴² See 5 U.S.C. § 46(j)(7).

¹⁴³ See U.S. Dept. of State, State Sponsors of Terrorism, [State Sponsors of Terrorism - United States Department of State](https://www.state.gov/sponsors-of-terrorism/) (last accessed Sept. 26, 2023).

¹⁴⁴ For example, the United Nations Conference on Trade and Development (UNCTAD) Intergovernmental Experts Group on Consumer Protection Law and Policy; Organisation for Economic Co-operation and Development (OECD) Committee on Consumer Policy (2013-22); Asia Pacific Economic Cooperation forum (APEC); and Global Privacy Assembly (GPA) (formerly the International Conference of Data Protection and Privacy Commissioners).

¹⁴⁵ The FTC also has contacts with Chinese agencies on competition matters; those interactions are not addressed in this report.

¹⁴⁶ See Press Release, FTC, FTC Signs Memorandum of Understanding with China’s Consumer Protection Agency (June 12, 2007), <https://www.ftc.gov/news-events/news/press-releases/2007/06/ftc-signs-memorandum-understanding-chinas-consumer-protection-agency>.

some fabricated problem. The callers demanded large amounts of money to resolve the issue, and the FTC received hundreds of complaints on this subject. The FTC issued a warning in both English and Chinese alerting people to the scams.¹⁴⁷ Staff also worked with Chinese Embassy officials to post warnings in English and Chinese about the scams and linking to the FTC's website for further information.¹⁴⁸ The issue received substantial media coverage.¹⁴⁹

More recently, the FTC published an advisory (in English and Chinese) regarding a new investment scam targeting WeChat groups. According to the FTC the scam “stole millions from the Chinese community in the U.S.”:

Using WeChat groups, scammers heavily promoted the investment with pictures and stories about supposed successful investors. To invest, people agreed to over-pay upfront — as much as three times the retail price — to buy items like iPhones, laptops, and furniture. In exchange, scammers promised to return investors' money in 1-3 months. And, as a thank you for investing, investors got to keep the products for free. At first, scammers shipped products and paid out some investors, leading people to sink more money into the scheme. In truth, there was no investment and what little scammers paid out was money they stole from new investors.¹⁵⁰

FTC staff has informed Chinese Embassy staff of this advisory.

The FTC has also interacted with various Chinese agencies on privacy and data security, in coordination with other U.S. government agencies. This includes interactions with (a) the Ministry of Industry and Information Technology (MIIT) (on the FTC's general approach to privacy enforcement); (b) the Ministry of Commerce (MOFCOM) (on a wide variety of issues, including multilevel marketing, financial consumer protection, commercial data security, breach notification, and e-commerce, as well as on China's participation in the APEC Cross-Border Privacy Rules (CBPR) System); and (c) the Cyberspace Administration of China (CAC) (on China's draft cybersecurity law). In 2019 FTC staff also provided materials and presentations at Beijing Normal University about enforcement of the Children's Online Privacy Protection Act (COPPA), which can apply to entities outside the United States.¹⁵¹ These interactions, however, did not involve requests for enforcement cooperation in specific matters.

¹⁴⁷ See Pati Poss, FTC, Scammers impersonate the Chinese Consulate (Apr. 18, 2018), <https://www.consumer.ftc.gov/blog/2018/04/scammers-impersonate-chinese-consulate>.

¹⁴⁸ See, e.g., Embassy of the People's Republic of China in the United States of America, Phone Scam Alert (Apr. 19, 2018 12:00 pm), http://us.china-embassy.gov.cn/eng/notices/201804/t20180419_4409167.htm.

¹⁴⁹ See, e.g., Natt Garun, The Verge, The FTC warns of robot calling spam targeting Chinese speakers (Apr. 22, 2018), <https://www.theverge.com/2018/4/22/17267970/ftc-robot-scam-call-fraud-chinese-embassy-consulate-212-244>.

¹⁵⁰ See Tiffany Smedley, FTC, Investment scam targeting WeChat groups (May 18, 2023), https://consumer.ftc.gov/consumer-alerts/2023/05/investment-scam-targeting-wechat-groups?utm_source=govdelivery.

¹⁵¹ See FTC, Complying with COPPA: Frequently Asked Questions, <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions> (last accessed Sept. 26, 2023) (“Foreign-based websites and online services must comply with COPPA if they are directed to children in the United States, or if they knowingly collect personal information from children in the U.S. The law’s definition of “operator” includes foreign-based websites and online services that are involved in commerce in the United States or its territories. As a related matter, U.S.-based sites and services that collect information from foreign children also are subject to COPPA.”)

IV. Consumer Complaint Data and Trends Related to Ransomware, Tech Support Scams, and China, Russia, North Korea, and Iran

While the FTC receives millions of reports about fraud, including cross-border fraud,¹⁵² consumer reports about ransomware and other cyber-related attacks comprise only a small fraction of those reports. And, except for China, when consumers file complaints they rarely mention the other countries identified in the RANSOMWARE Act—namely, Russia, North Korea, and Iran.

Between January 1, 2019, and June 30, 2023, the FTC received over 11 million consumer fraud reports, over one million of which (nearly 10%) were cross border.¹⁵³ These reports show that U.S. consumers encounter significant fraud from outside the United States, with more than 270,000 consumers reporting an incident of cross-border fraud during this period. U.S. consumers also suffer significant injury from cross-border fraud—over \$2.1 billion during this period and over \$4.4 billion since 2006.¹⁵⁴

As detailed below and in the FTC's October 2023 report, "The U.S. SAFE WEB Act and the FTC's Fight Against Cross-Border Fraud," consumer reports show that China is a leading source of cross-border complaints. Those complaints, however, rarely concern ransomware or other cyber-related attacks.¹⁵⁵ Between January 1, 2019, and June 30, 2023, the FTC received 89,450 reports about fraud originating in China, but *less than 1%* of these reports (0.31%) related to ransomware or other computer exploits. And while consumers report slightly more incidents of tech support scams—a type of fraud akin to ransomware—such reports comprise *less than 2%* (1.89%) of the fraud reports about China during this period. Instead, when consumers report about fraud originating in China, they are largely concerned with issues related to online shopping, which account for *over 55%* of all such complaints.¹⁵⁶

Consumers have also reported misconduct they believe originated in Russia, Iran, and North Korea, but to a lesser extent than China. This lesser reporting is especially true for North Korea and Iran. *Combined*, consumers have filed 7,036 fraud reports about these three countries between January 1, 2019, and June 30, 2023—*.063% of all fraud reports* received by the FTC during this period. When consumers do report about harmful conduct originating in these countries, it is not uncommon to see reports about tech support scams, especially from Russia since 2022, but reports about malware and other computer exploits are rare for all three countries.

This scarcity of consumer complaints about ransomware and other computer exploits is not surprising. As a general matter, the FTC receives few complaints about ransomware or other computer exploits, especially when compared to other types of reported fraud. In the four and a half years since January 1,

¹⁵² The FTC retains fraud reports in Consumer Sentinel – a secure online database available only to registered law enforcement agencies and users. *See infra* [Section IV.A](#). Consumer Sentinel has a five-year data retention policy, with reports older than five years purged biannually. In drafting this report, the FTC relied on Sentinel data for January 1, 2019, to June 30, 2023 (loaded September 6, 2023).

¹⁵³ The FTC considers a report to be "cross-border" when the consumer country is provided and the company country is provided, and those countries are different.

¹⁵⁴ *See also* FTC 2023 SAFE WEB Report.

¹⁵⁵ China includes reports about Hong Kong and Macau, which are tracked separately in Consumer Sentinel.

¹⁵⁶ *See also* Section I and Appendix A of the FTC's 2023 SAFE WEB Report.

2019, only 1.40% of all fraud reports have concerned such issues. And, when reporting about such attacks, the majority of U.S. consumers—over 92%—report that the attack either originated within the United States or do not report a location.

Reports about tech support scams are more prevalent—4.0% of all fraud reports—but only some of those reports may involve actual ransomware. Similarly, when reporting about tech support scams, the vast majority of U.S. consumers—over 95%—also either identify the United States as the country of origin or do not report the origin country. In addition, when U.S. consumers do identify a foreign source of tech support fraud, which unlike ransomware attacks often involves telemarketing, they most frequently identify India as the source of cross-border tech support fraud. This trend is not new and underscores why the FTC has devoted enforcement resources to tech support scams, including those originating overseas, *see supra* [Section I.B](#), and has worked with authorities in India and elsewhere to crack down on such scams.¹⁵⁷

Below we provide a detailed analysis of complaints collected in Consumer Sentinel related to ransomware, malware and other computer exploits, and tech support scams, as well as complaints related to entities¹⁵⁸ that consumers report as being located in China, Russia, North Korea, or Iran. When reviewing this information, it is important to note that the volume of consumer reports and the reported origins of fraud could be influenced by several important factors. First, as a general matter, consumers often do not file complaints, especially with the government.¹⁵⁹ And, even when consumers do file complaints, the FTC may not receive them. Consumer Sentinel is a powerful database for fraud and other consumer protection complaints with many important data contributors, but it is not a central repository for all consumer protection or cyber security complaints.¹⁶⁰ In addition, consumers typically do not know where the entities perpetrating these attacks are located. As a general matter, foreign

¹⁵⁷ *See, e.g., FTC v. Pecon Software Ltd.*, No. 12-cv-7186 (S.D. NY., Sept. 24, 2012), available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/1123118-pecon-software-ltd-et-al>; *FTC v. Lakshmi Infosoul Services Pvt Ltd.*, 12-cv-191 (S.D. NY, Sept., 24, 2012), available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/1223245-lakshmi-infosoul-services-pvt-ltd>. *See also* Press Release, FTC, FTC and Federal, State and International Partners Announce Major Crackdown on Tech Support Scams (May 12, 2017), <https://www.ftc.gov/news-events/news/press-releases/2017/05/ftc-federal-state-international-partners-announce-major-crackdown-tech-support-scams>.

¹⁵⁸ In this report, “entities” refers to both companies and individuals.

¹⁵⁹ *See, e.g.,* Keith B. Anderson, To Whom Do Victims of Mass-Market Consumer Fraud Complain? (May 24, 2021), available at <https://ssrn.com/abstract=3852323> or <http://dx.doi.org/10.2139/ssrn.3852323> (finding that, based on data from surveys of mass-market consumer fraud sponsored by the FTC in 2005, 2011, and 2017, in about 45% of instances, victims complained to someone beyond their family or friends, most frequently to someone directly involved in the transaction, such as the seller or manufacturer, a bank, or credit card company, but only 4.8% of victims complained to a BBB or government agency).

¹⁶⁰ *See, e.g.,* FBI, Internet Crime Complaint center, <https://www.ic3.gov/Home/ComplaintChoice> (last accessed Sept. 28, 2023). As noted above, the FBI positions itself as the lead federal agency for investigating cyber-attacks and intrusions. *See* FBI, What We Investigate, <https://www.fbi.gov/investigate/cyber> (last accessed Sept. 28, 2023). Another important source of possible ransomware complaints is the Microsoft Corporation Cyber Crime Center, a Sentinel data contributor, and the Cybercrime Support Network, which refers consumers to [ReportFraud.ftc.gov](https://www.ftc.gov/ReportFraud). The FBI’s IC3 also prepares annual reports summarizing its complaints. *See* FBI, Internet Crime Complaint Center, Annual Reports, <https://www.ic3.gov/Home/AnnualReports> (last accessed Sept. 28, 2023). The following summarizes the number of ransomware complaints received with adjusted monetary losses: 2019 (2,047 complaints and losses of over \$8.9 million); 2020 (2,474 complaints and losses of over \$29.1 million); 2021 (3,729 complaints and losses of over \$49.2 million); and 2022 (2,385 complaints and losses of \$34.3 million). *Id.*

scammers often mislead consumers about or conceal their locations through various techniques.¹⁶¹ This is likely even more typical for criminal enterprises that initiate cyber-attacks. Last, with respect to insufficient data security practices, which are an important component of the FTC's data security enforcement program, the average consumer is unlikely to know if a company's data security practices have contributed to a cyber-attack. Consequently, while consumer reports are a common way that the FTC identifies targets for many fraud enforcement actions, they are not a leading source of information for its data security enforcement program.

A. The Consumer Sentinel Network

Consumer complaints (also called reports), are essential to the FTC's enforcement efforts, providing direct information about fraud and other harms that consumers encounter in the marketplace. The FTC regularly uses consumer complaints to identify enforcement targets and in enforcement actions and uses aggregate complaint data to report publicly on trends.¹⁶² However, the FTC does not act upon each individual complaint received, directly or indirectly, given the millions of consumer complaints received each year. The FTC's companion SAFE WEB report to Congress describes this system in greater detail.

The FTC receives complaints directly from consumers via its web-based complaint portal ReportFraud.ftc.gov and phone calls to the FTC's Consumer Response Center.¹⁶³ The FTC also receives consumer reports from other federal, state, local, and foreign law enforcement agencies, and certain organizations.¹⁶⁴ The FTC retains this data in the Consumer Sentinel Network, a secure online database available only to registered law enforcement agencies and users.¹⁶⁵ The fraud complaints housed in Sentinel are currently categorized into 17 categories and 46 subcategories.¹⁶⁶

B. Consumer Sentinel Complaints about Malware and Tech Support Scams

The Consumer Sentinel subcategories of "Malware & Computer Exploits" and "Tech Support Scams" are relevant to this report. Ransomware, a specially designed variant of malware that holds data hostage pending payment, is only one of the malware variants reported under this subcategory. The subcategory of "Malware & Computer Exploits" also includes consumer complaints about spyware, adware, and other types of malware, as well as denial of service attacks, some of which may be beyond the scope of

¹⁶¹ See FTC 2023 SAFE WEB Report at 6 (noting that foreign scammers often mislead consumers about or conceal their locations, including by using phone numbers that appear to be from the United States, VoIP technology such as spoofing, fake social media profiles, and other tactics).

¹⁶² Additional information on how the FTC uses consumer complaints is located in Appendix B of the FTC's 2023 SAFE WEB Report.

¹⁶³ Consumers can also report identity theft at IdentityTheft.gov and unwanted calls to the National Do Not Call Registry at donotcall.gov.

¹⁶⁴ A complete list of Sentinel data contributors is available at FTC, Consumer Sentinel Network Data Contributors, <https://www.ftc.gov/enforcement/consumer-sentinel-network/data-contributors> (last accessed Sept. 28, 2023).

¹⁶⁵ See FTC, Consumer Sentinel Network, <https://www.ftc.gov/enforcement/consumer-sentinel-network> (last accessed Sept. 28, 2023).

¹⁶⁶ Sentinel category descriptions are available at FTC, Consumer Sentinel Network, https://www.ftc.gov/system/files/attachments/data-sets/category_definitions.pdf (last accessed Sept. 28, 2023). Sentinel subcategory definitions are available at FTC, Consumer Sentinel Network Subcategory Definitions (May 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/CSNPSCFullDescriptions.pdf.

Congress's inquiry.¹⁶⁷ The subcategory of "Tech Support Scams" includes complaints about scammers who claim to be computer technicians associated with a well-known company or its products; not all of these scams, as noted above, necessarily involve computers actually taken hostage.¹⁶⁸ Thus, while fraud is generally underreported, complaints under both of these categories cannot be relied upon to accurately measure ransomware fraud.¹⁶⁹

1. Malware and Computer Exploits

The FTC has received relatively few consumer reports about malware and computer exploits, cross-border or otherwise. During the four and a half years January 1, 2019, to June 30, 2023, the FTC received 154,911 such reports, about a quarter of which were cross-border. Consumer complaints about such attacks and exploits accounted for *only 1.40%* of the fraud complaints the FTC collected during this period.

When consumers do report about such attacks, the vast majority—at least 92%—report that the attack either originated from the United States or do not report a location.¹⁷⁰ (See *Figure 1*.) When U.S. consumers report that malware or other computer exploits have originated abroad, the most common country that they report is the Philippines, which is identified in 3,361 complaints (36.8% of U.S. consumer cross-border complaints and 2.74% of all U.S. consumer complaints) since January 1, 2019. Other reported countries include Côte d'Ivoire, which was identified by U.S. consumers in 1,165 complaints (12.8% of U.S. consumer cross-border complaints and 0.95% of all U.S. consumer complaints), and Nigeria, which U.S. consumers identified in 610 complaints (6.7% of U.S. consumer cross-border complaints and 0.50% of all U.S. consumer complaints).

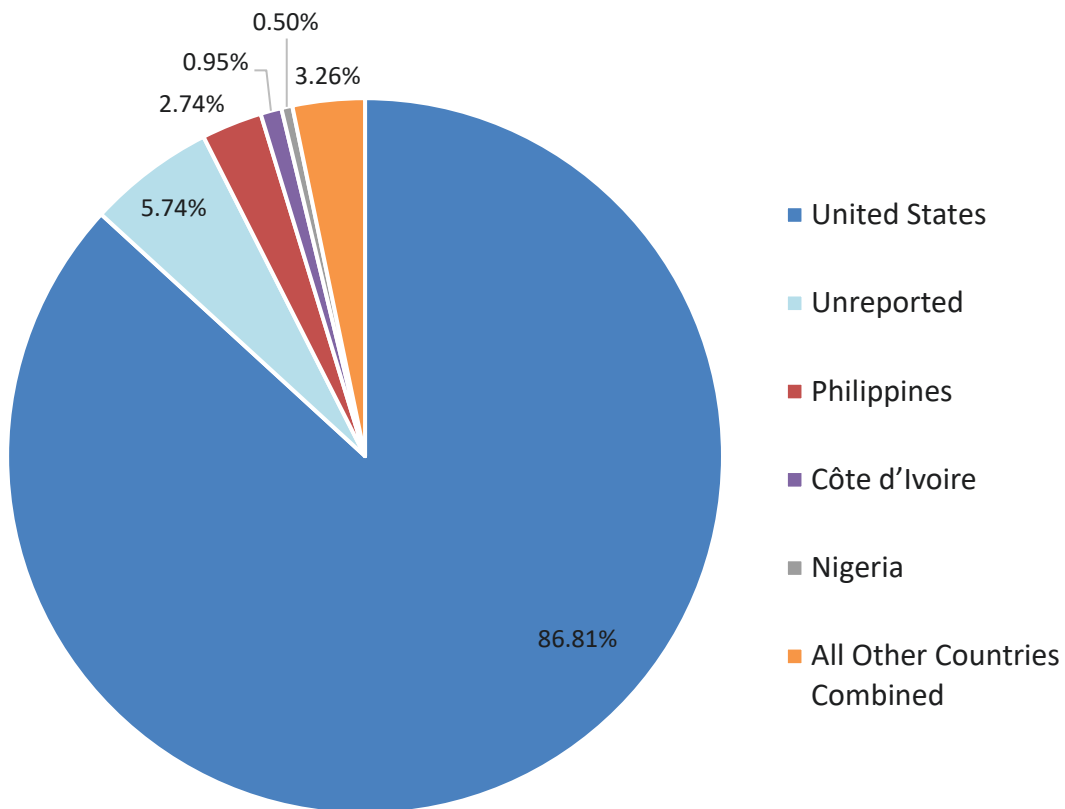
¹⁶⁷ The subcategory of "Malware & Computer Exploits" is defined as "complaints about computer software that gathers consumer information without consumer knowledge and/or consent. Spyware receives information about consumers, including browsing and internet usage habits. Adware displays advertising banners, re-directs consumers to websites, and conducts other forms of advertising. Malware is malicious software that harms consumers' computers or software. Malware includes viruses, Trojans, and worms, as well as ransomware, a specially designed variant of malware that holds data hostage pending payment. This category also includes denial of service attacks that flood websites with connection requests, as well as botnets that control computers like puppets." The subcategory is part of a larger category of complaints about "Privacy, Data Security, and Cyber Threats," along with reports for the subcategory of "Privacy & Data Security."

¹⁶⁸ The subcategory of "Tech Support Scams" is defined as "Complaints about a scammer who claims to be a computer technician associated with a well-known company or its products. This individual will say viruses or other malware have been detected on consumers' computers and that remote access is needed for diagnosis/repair; ultimately, the "tech" will give a sales pitch for unnecessary software services, like virus removal. The scammer might also steal any personal information on the victim's computer." "Tech support scams" are part of the broader category of "Imposter scams," which also includes romance scams, and government, business, and family & friend imposter scams.

¹⁶⁹ When consumers report identity theft, they will occasionally note that they have been the victim of a ransomware attack or that a company with which they have done business notified them that it was subject to a ransomware attack. Of the over 5 million reports of identity theft the FTC received between January 1, 2018, and December 31, 2022, less than 1,000 of them included the phrase "ransom." Of these, four consumers identified either China or Russia as the country of origin.

¹⁷⁰ When reporting about such frauds, 92.7% of all consumers and 92% of U.S. consumers either report the United States as the source of the fraud or do not report a location.

Figure 1: Top Country for Malware & Computer Exploits Complaints as Reported by U.S. Consumers



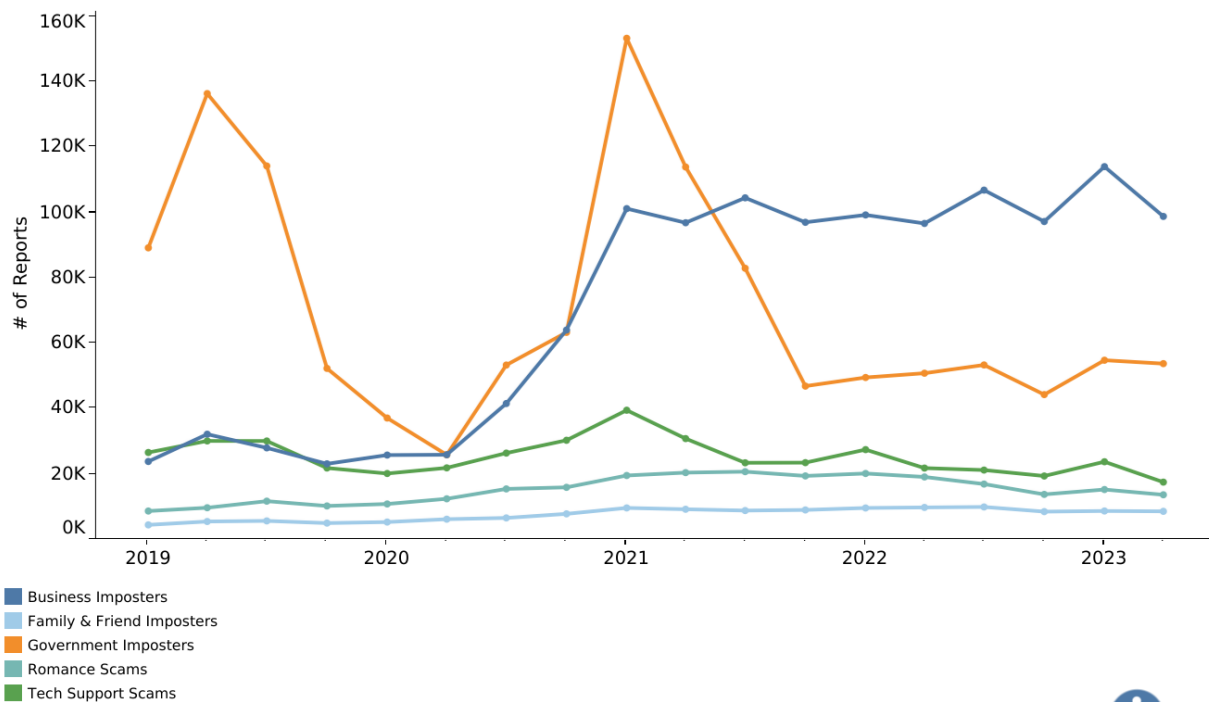
2. Tech Support Scams

Collectively, imposter scams—a general category of fraud complaints where someone pretends to be a trusted person to get consumers to send money or give personal information—are the most common category of fraud reported by consumers since January 1, 2019.¹⁷¹ Tech Support Scams is a subcategory of imposter scams along with romance scams, business, government, and family and friend imposter scams. While a relatively consistent type of fraud, tech support scams are less common than other types of imposter scams. (See Figure 2.) Since January 1, 2019, the FTC received 8,611 reports about tech support scams, 9% of all fraud reports for this period. Of these reports, 20.2% of them were cross-border and 68.5% were filed by U.S. consumers.

¹⁷¹ During this period, consumers reported 3,313,450 incidents of imposter scams, 29.9% of all fraud reports received by the FTC. Collectively, when consumers report about imposter frauds, most (between 77% and 86% each year) do not report a financial loss. Those who do, however, report median losses ranging from \$798 to \$1,000.

Figure 2: Reported Subcategories Over Time

FTC CONSUMER SENTINEL NETWORK

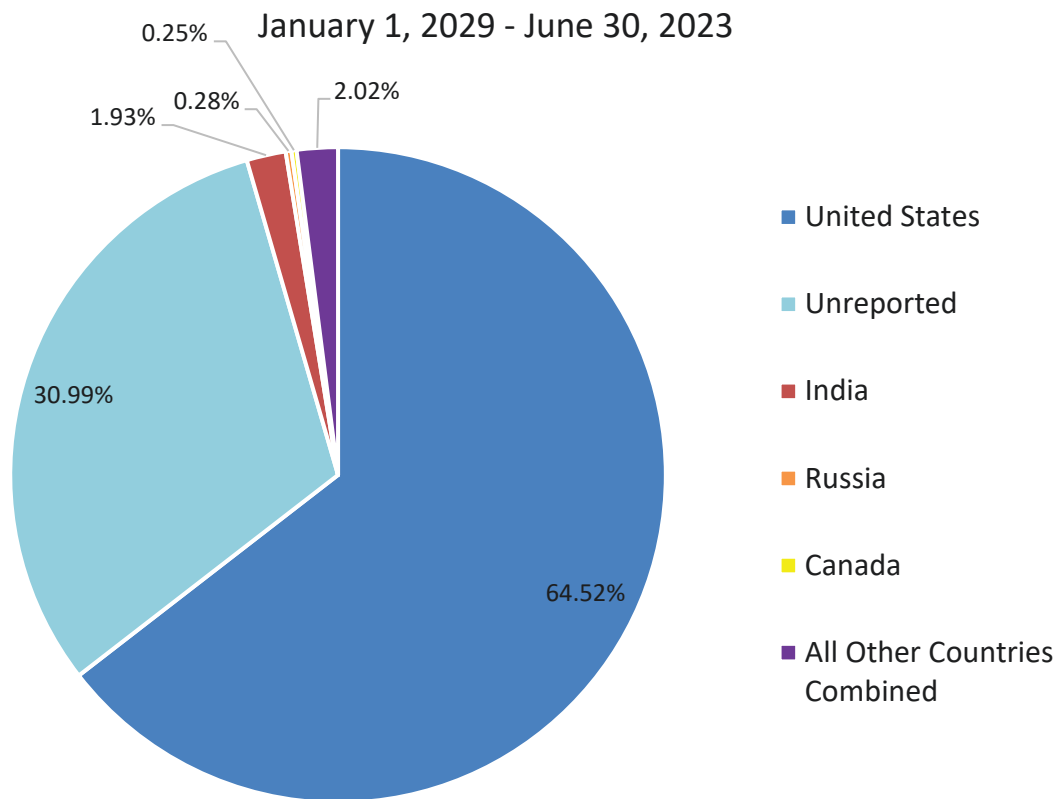
Published July 25, 2023
(data as of June 30, 2023)Report Subcategories
Category: Imposter ScamsView
Line GraphCategory
Imposter Scams
Subcategory
All

Unspecified reports not included.

FEDERAL TRADE COMMISSION • ftc.gov/exploredata

Similar to consumer complaints about malware & other computer exploits, most consumers who report about tech support scams either report that the perpetrator was located in the United States or do not report a location. When considering all tech support complaints, 80.3% of consumers report the location as the United States or do not report a location. The overwhelming majority of American consumers—95.5%—report that the scam originated in the United States or did not report a location. (See Figure 3.) It may be that consumers report a U.S. source because the scam often involves impersonating well known U.S. technology companies.

Figure 3: Top Countries for Tech Support Scam Complaints as Reported by U.S. Consumers



When U.S. consumers do report that a tech support scam originated abroad, they most commonly report that the fraud originated in India, which consumers identify in 3 % of their *cross-border* fraud reports. This is not surprising, as telemarketing boiler rooms in India have been a known source of such fraud for many years.¹⁷² Other countries that have been associated with tech support scams include Russia and Canada, *see supra* Figure 3 and *infra* Section IV.C. In total, U.S. consumers filed 13,810 cross-border reports about tech support scams since January 1, 2019.

C. Consumer Sentinel Complaints about China, Russia, North Korea, and Iran

A detailed analysis of Consumer Sentinel complaints where consumers have identified China, Russia, North Korea, or Iran as the location of the entity that perpetrated the attack appears below. As already

¹⁷² See *supra* Section I.B; see also, e.g., Press Release, U.S. Attorney's Office, District of New Jersey, Six Individuals Charged in Multimillion-Dollar Transnational Tech Support Scam Targeting Tens of Thousands of U.S. Victims (Dec. 16, 2022), <https://www.justice.gov/usao-nj/pr/six-individuals-charged-multimillion-dollar-transnational-tech-support-scam-targeting>.

noted, China is a leading source of cross-border complaints by U.S. consumers, and the FTC receives relatively few complaints related to Russia, Iran, or North Korea.

1. China

Between January 1, 2019, and June 30, 2023, consumers reported 89,450 incidents of fraudulent business conduct originating in China. The vast majority of these reports (96%) were cross-border, with 67,134 (75%) having been filed by U.S. consumers.¹⁷³ Consumer reports about fraud from China are varied, covering nearly all fraud subcategories tracked by the FTC.¹⁷⁴

With respect to the fraud subcategories relevant to Congress's inquiry, consumers have reported some incidents of tech support scams, and malware or other computer exploits, but such reports are few, comprising *only* 2.2% of reports about entities in China during this period, combined. Instead, when consumers report about fraud from China, most complaints, over 55%, are concerned with frauds related to online shopping, such as undisclosed costs, undelivered merchandise, and the failure to deliver ordered merchandise. (See Figure 4.) U.S. consumers have filed 255 reports about malware and computer exploits and 691 reports of tech support scams originating in China during this period.¹⁷⁵

Figure 4: Consumer Sentinel Reports about Entities in China

Rank	Sentinel Fraud Subcategory	Count	Percentage of Complaints
1	Online Shopping	49,569	55.4%
2	Other Miscellaneous	23,838	26.6%
3	Miscellaneous Investments & Investment Advice	5,947	6.6%
4	Business Imposters	3,406	3.8%
5	Social Networking Services	2,354	2.6%
6	Romance Scams	1,782	2.0%
7	Tech Support Scams	1,691	1.9%
8	Unsolicited Email	842	0.9%
9	Government Imposters	770	0.9%
10	Job Scams & Employment Agencies	575	0.6%
	...		
14	Malware & Computer Exploits	280	0.31%

¹⁷³ Of the complaints filed about entities in China, 799 (.9%) were filed by consumers who reported being in China, 2,885 (3.2%) did not report their location, and 67,134 (75%) were filed by consumers who reported being in the United States. The remaining 18,632 (20.8%) of complaints were cross-border complaints filed by foreign consumers.

¹⁷⁴ Also see Appendix A of the FTC's 2023 SAFE WEB Report.

¹⁷⁵ Because consumers can identify multiple subcategories when filing a complaint, adding these figures may not reflect the total number of consumer complaints for these two categories combined.

2. Russia

Between January 1, 2019, and June 30, 2023, the FTC received 6,160 complaints about entities located in Russia. Of these reports, 5,279 (85.7%) were cross-border, with 2,998 (48.7%) having been filed by U.S. consumers.¹⁷⁶ To put this number in context, U.S. consumers filed more than 22 times as many complaints against Chinese businesses during the same period.

Consumer complaints about Russia are varied, covering most identified Sentinel fraud subcategories, such as tech support and other imposter scams, online shopping, unsolicited emails and text messages, and frauds related to miscellaneous investments and advice. During this period, tech support scams represented almost a third of these complaints – a total of 1,965 (31.9%). (See Figure 5.) A majority of these complaints (77%) were filed *in the last year and a half*—since January 1, 2022.¹⁷⁷ For the same period, the FTC received 119 complaints (1.9%) from consumers about malware and other computer exploits originating in Russia. Specifically, U.S. consumers filed 102 reports about malware and computer and 865 reports of tech support scams originating in Russia since 2019.¹⁷⁸

Figure 5: Consumer Sentinel Reports about Entities in Russia

Rank	Sentinel Fraud Subcategory	Count	Percentage of Complaints
1	<i>Tech Support Scams</i>	1,965	31.9%
2	Romance Scams	880	14.3%
3	Online Shopping	802	13.0%
4	Unsolicited Email	549	8.9%
5	Miscellaneous Investments & Investment Advice	460	7.5%
6	Business Imposters	446	7.2%
7	Other Miscellaneous	438	7.1%
8	Unsolicited Text Messages	159	2.6%
9	Government Imposters	145	2.4%
10	Unwanted Telemarketing Calls	144	2.3%
11	<i>Malware & Computer Exploits</i>	119	1.9%

¹⁷⁶ Of the complaints filed about entities in Russia, 343 (5.6%) were filed by consumers who reported being in Russia, 538 (8.7%) did not report their location, and 2,998 (48.7%) were filed by consumers who reported being in the United States. The remaining 2,281 (37%) were cross-border complaints filed by foreign consumers.

¹⁷⁷ In 2022, consumers submitted 816 complaints about tech support scams that identified Russia and the country of origin, and 698 in the first half of 2023.

¹⁷⁸ As noted above, because consumers can identify multiple subcategories when filing a complaint, adding these figures may not reflect the total number of consumer complaints for these two categories combined.

3. North Korea

Between January 1, 2019, and June 30, 2023, consumers reported 490 incidents of fraud originating in North Korea. Of these reports, 440 reports (89.8%) were cross-border, with 274 (55.9%) having been filed by U.S. consumers.¹⁷⁹

The only complaint category to exceed 100 complaints was online shopping, with 122 complaints (24.9%) during the four-and-a-half-year period. During this period, consumers filed 71 reports about tech support scams and 12 reports about malware or other computer exploits. (See Figure 6.)

Specifically, during this period, U.S. consumers filed 43 reports about tech support scams and eight about malware and other computer exploits that they reported as having originated in North Korea.¹⁸⁰

Figure 6: Consumer Sentinel Reports about Entities in North Korea

Rank	Sentinel Fraud Subcategory	Count	Percentage of Complaints
1	Online Shopping	122	24.9%
2	Romance Scams	72	14.7%
3	<i>Tech Support Scams</i>	71	14.5%
4	Miscellaneous Investments & Investment Advice	69	14.1%
5	Business Imposters	30	6.1%
6	Job Scams & Employment Agencies	25	5.1%
7	Other Miscellaneous	25	5.1%
8	Unsolicited Email	16	3.3%
9	Government Imposters	14	2.9%
10	<i>Malware & Computer Exploits</i>	12	2.4%

¹⁷⁹ Of the complaints filed about entities located in North Korea, 31 (6.3%) were filed by consumers who reported being from North Korea, 19 (3.9%) were filed by consumers who did not report their location, and 274 (55.9%) were filed by consumers who reported being in the United States. The remaining 166 (33.9%) were cross-border complaints filed by foreign consumers.

¹⁸⁰ As noted above, consumers are often unaware of the source of fraud. See *supra* [Section IV](#). In addition, the common language shared by North Korea and South Korea, and the similar formal country names (respectively, the “Democratic People’s Republic of Korea” and the “Republic of Korea”), may result in some misreporting with respect to fraud associated with these two countries.

4. Iran

The FTC received 386 complaints about businesses located in Iran between January 1, 2019, and June 30, 2023. Of these reports, 258 (66.8%) were cross-border, with 185 (47.9%) having been filed by U.S. consumers.¹⁸¹

No reporting subcategory received over 100 complaints during this period. During this period, consumers filed 67 reports (17.4%) about tech support scams and 16 reports (4.1%) about malware and other computer exploits that they believed originated in Iran. (See Figure 7.)

Figure 7: Consumer Sentinel Reports about Entities in Iran

Rank	Sentinel Fraud Subcategory	Count	Percentage of Complaints
1	Romance Scams	81	21.0%
2	<i>Tech Support Scams</i>	67	17.4%
3	Business Imposters	49	12.7%
4	Miscellaneous Investments & Investment Advice	42	10.9%
5	Unsolicited Email	40	10.4%
6	Government Imposters	34	8.8%
7	Unwanted Telemarketing Calls	32	8.3%
8	Online Shopping	23	6.0%
9	<i>Malware & Computer Exploits</i>	16	4.1%
10	Job Scams & Employment Agencies	10	2.6%

V. Legislative and Business Recommendations

The FTC here submits recommendations as directed by the RANSOMWARE Act.

First, the FTC again encourages Congress to make the U.S. SAFE WEB Act permanent. As detailed in the FTC's 2023 SAFE WEB Report, a lapse of such legislation would deprive the FTC of its clear authority to pursue fraudulent and other harmful conduct relating to foreign commerce, likely having a dramatic impact on U.S. consumers. It would also hinder the FTC's ability to obtain assistance from and provide assistance to foreign partners—vital components of cross-border cooperation. Such information sharing and enforcement cooperation helps the FTC to better combat cross-border fraud and other harms. Without SAFE WEB, the FTC's ability to work with international partners, such as its coordination with Australia, Canada, and the United Kingdom in *Pecon Software*, would be significantly curtailed.

¹⁸¹ Of the complaints filed about entities located in Iran, 79 (20.5%) were filed by consumers who reported being from Iran, 49 (12.7%) did not report their location, and 185 (47.9%) reported being located in the United States. The remaining 73 (18.9%) were reported by foreign consumers.

In addition, the FTC urges Congress to amend Section 13(b) of the FTC Act¹⁸² to restore the FTC's ability to provide refunds to harmed consumers and prevent violators from keeping the money they earned by breaking the law. In April 2021, the Supreme Court issued its decision in *AMG Capital Management v. FTC*, which overturned four decades of circuit court precedent and held that Section 13(b) of the FTC Act no longer allowed courts to order defendants to pay refunds to harmed consumers or order defendants to disgorge their unjust gains.¹⁸³ That decision has significantly hampered the FTC's ability to get harmed consumers their money back and prevent wrongdoers from profiting from their violations of the FTC Act.¹⁸⁴ As the Commission has stated in previous testimony, restoring the FTC's ability to use Section 13(b) to obtain court orders requiring companies to pay equitable monetary relief is critical to the agency's ability to protect consumers from cross-border fraud.

The Commission also continues to urge Congress to enact privacy and data security legislation, enforceable by the FTC, as a key component of advancing the security of the United States and U.S. companies against ransomware and other cyber-related attacks. The FTC most recently reported to Congress on privacy and security in 2021, noting its enforcement actions against companies that engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data.¹⁸⁵ In that report, the Commission expressed its hope that comprehensive federal privacy and data security legislation would, among other things, expand the agency's civil penalty authority, APA rulemaking authority, and jurisdiction over non-profits and common carriers.¹⁸⁶

Finally, businesses often serve as the front-line defenses against cyber attacks and are responsible for engaging in reasonable practices to safeguard customer data. As a result, one of the most important ways to fight ransomware attacks is for businesses to take appropriate data security steps to protect themselves and the data in their possession. The FTC's "Start with Security" Business Education materials discuss several foundational principals that businesses should follow to better protect their customer's data, including counseling companies to 1) avoid collecting personal data they do not need; 2) retain information only so long as there is a legitimate business need; 3) do not use personal data that's not necessary; 4) restrict access to sensitive data; 5) limit administrative access; 6) insist on complex and unique passwords; 7) store passwords securely; 8) store personal information securely and protect it during transmission; 9) segment your network and monitor who's trying to get in and out; 10) secure remote access to your network; 11) apply sound security practices when developing new products, including training staff, verifying security features work and testing for common vulnerabilities; 12)

¹⁸² 15 U.S.C. § 53(b).

¹⁸³ *AMG Capital Mgmt., LLC v. FTC*, 141 S. Ct. 1341 (Apr. 22, 2021).

¹⁸⁴ See, e.g., Press Release, FTC, FTC Order to Bar ZyCal Bioceuticals from Deceptive Health Marketing (Feb. 6, 2023), <https://www.ftc.gov/legal-library/browse/cases-proceedings/182-3133-zycal-bioceuticals-healthcare-company-inc> ("Unfortunately, the Supreme Court decision in *AMG Capital Management* prevented us from obtaining refunds for consumers in this case. The Commission has urged Congress to enact legislation to restore the agency's ability to obtain critical relief for consumers through federal court actions."); Press Release, FTC, Federal Court Rules in Favor of FTC, Halting Illegal Tactics Used to Promote Smoking Cessation, Weight-Loss, and Sexual-Performance Aids (Mar. 25, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/03/federal-court-rules-favor-ftc-halting-illegal-tactics-used-promote-smoking-cessation-weight-loss> ("[D]espite the fact that the FTC presented evidence that consumers lost \$18.2 million to the defendants' deceptive marketing, the court declined to order any compensation because of [the] Supreme Court's ruling in the case of *AMG v. FTC*, which undercuts the agency's authority to obtain such consumer redress.")

¹⁸⁵ See FTC Report to Congress on Privacy and Security (Sept. 13, 2021) at Appendix pp3-5, available at https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf

¹⁸⁶ *Id.* at p. 10.

make sure service providers implement reasonable security measures; 13) put procedures in place to keep your security current and address vulnerabilities that may arise; 14) secure paper, physical media, and devices; and 15) dispose of sensitive data securely.¹⁸⁷ More recently, the FTC has also developed specific guidance for App developers, buyers and sellers of consumer debt, businesses collecting consumer health information, DNA companies, and financial institutions.¹⁸⁸ With regard to ransomware specifically, businesses need to train their employees to recognize and avoid phishing emails with links or attachments, which make up the majority of ransomware attacks. They should also invest in additional means of protection, like email authentication, and intrusion prevention software, and set them to update automatically. Businesses should also consider regularly backing up their data to drives or servers that are not connected to the internet. Because no security system can prevent all attacks, though, business should also have a plan in place to quickly respond to potential ransomware attacks in order to respond quickly to mitigate the damage they can cause.

¹⁸⁷ See FTC, Start With Security, A Guide for Business (Jun. 2015), *available at* <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>; FTC, Start with Security: A Guide for Business, <https://www.ftc.gov/business-guidance/resources/start-security-guide-business> (last accessed Oct. 2, 2023).

¹⁸⁸ See FTC, Data Security, <https://www.ftc.gov/business-guidance/privacy-security/data-security> (last accessed Oct. 2, 2023).

Acknowledgments

This report was drafted by Stacy Procter, Angel Martinez, Olivia Barney-Fishbein, and Laureen Kapin of the FTC's Office of International Affairs. Additional acknowledgement goes to Paul Witt, Elizabeth Anne Miles, and Nicholas Mastrocinque of the FTC's Division of Consumer Response and Operations, Michael Panzera of the FTC's Office of International Affairs, and the staff of the FTC's Bureau of Consumer Protection.