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

Update: 2025

A Report to Congress

January 30, 2026

FEDERAL TRADE COMMISSION

Andrew N. Ferguson, Chairman
Mark R. Meador, Commissioner

Contents

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" of 2023, also known as the RANSOMWARE Act.[1] The FTC protects consumers in an increasingly global and digital economy. Congress has authorized the FTC to pursue deceptive or unfair acts or practices involving foreign actors targeting Americans.[2] As part of that effort, the FTC plays an important role in protecting the public against ransomware and other cyber-related attacks, including by complementing the work of other U.S. government agencies in the greater fight against these threats.[3] The FTC pursues data security

---

[1] Consolidated Appropriations Act, 2023, Division BB, Title V, Public Law No: 117-328, *available at* https://www.congress.gov/117/plaws/publ328/PLAW-117publ328.pdf. 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 that the FTC 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 that could advance the security of the United States or U.S. companies, and recommendations for U.S. businesses and citizens to implement best practices to mitigate against such attacks. In addition to the original report, Congress requested in Section 503(a) that the FTC promulgate additional reports in 2025 and 2027.

[2] Section 3 of the SAFE WEB Act, codified at Section 5(a) of the FTC Act, 15 U.S.C. §45(a)(4)(A) (providing that "unfair and deceptive acts and practices" includes such acts or practices involving foreign commerce that "(i) cause or are likely to cause reasonably foreseeable injury within the United States; or (ii) involve material conduct occurring within the United States."). In 2023, the FTC concurrently submitted a companion report, The U.S. SAFE WEB Act and the FTC's Fight Against Cross-Border Fraud (Oct. 20, 2023) ("2023 SAFE WEB Report"), as required under Pub. L. No. 116-173, 134 Stat. 837 (2020), to update Congress on the implementation of the U.S. SAFE WEB Act of 2006, 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)). *See generally* 2023 SAFE WEB Report (Attachment B), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/ftc_safe_web_congressional_report_oct_2023.pdf.

[3] In addition to the FTC, U.S. law enforcement agencies leading the fight against ransomware include, for example, the Federal Bureau of Investigation (FBI); Department of Homeland Security, Cybersecurity & Infrastructure Security Agency (CISA); the U.S. Secret Service; the National Security Agency (NSA); the U.S. Department of Justice, Criminal Division; and the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN). *See, e.g.*, Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), Cybersecurity Unit (Dec. 1, 2025), https://www.justice.gov/criminal/criminal-ccips/cybersecurity-unit; 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 Nov. 25, 2025); CISA, Stop Ransomware, https://www.cisa.gov/stopransomware (last accessed Nov. 25, 2025); U.S. Secret Service, Investigations, Cyber Investigations, https://www.secretservice.gov/investigations/cyber (last accessed Nov. 25, 2025); U.S. Secret Service, Preparing for a Cyber Incident, https://www.secretservice.gov/investigations/cyberincident (last accessed Nov. 25, 2025); U.S. Secret Service, Ransomware, https://www.secretservice.gov/investigations/ransomware (last accessed Nov. 25, 2025); CISA, Alert, Joint Advisory Issued on Protecting Against Interlock Ransomware (Jul. 22, 2025), https://www.cisa.gov/news-events/alerts/2025/07/22/joint-advisory-issued-protecting-against-interlock-ransomware; FinCEN, Press Release, FinCEN Finds Cambodia-Based Huione Group to be of Primary Money Laundering Concern, Proposes a Rule to Combat Cyber Scams and Heists (May 01, 2025), https://www.fincen.gov/news/news-releases/fincen-finds-cambodia-based-huione-group-be-primary-money-laundering-concern ("Huione Group serves as a critical node for laundering proceeds of cyber heists carried out by [North Korea]…."); CISA, Cybersecurity Advisory, Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations (August 28, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a; NSA, Press Release, #StopRansomware Guide Released by NSA and Partners (May 23, 2023), https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3403814/stopransomware-guide-released-by-nsa-and-partners/.

enforcement to ensure that companies take reasonable 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 consumer complaints help the FTC and other enforcers spot trends and prioritize enforcement activities.

In 2023, the FTC submitted its first report required under the RANSOMWARE Act ("2023 Ransomware Report") (Attachment A).[4] The 2023 Ransomware Report sets forth a comprehensive historical overview of the FTC's activities as to ransomware and cyber-related attacks, and as to the four countries identified by the RANSOMWARE Act (China, Russia, North Korea, and Iran),[5] including consumer complaint data through June 30, 2023. The present report provides an update on those activities from July 1, 2023, through June 30, 2025 (the "reporting period"), as follows:

- 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 explains the FTC's enforcement work concerning tech support scams, which sometimes involve bad actors installing malware in consumers' computers. 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.[6]

- Section II describes additional FTC enforcement actions involving China and Russia, including those involving privacy, data security, and fraud issues.

- Section III addresses cross-border cooperation on the subjects described in the report.

- 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.

- Section V offers legislative recommendations related to the U.S. SAFE WEB Act to advance the FTC's mission 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's Efforts in the Greater Fight Against Ransomware and Cyber-Related Attacks (Oct. 20, 2023), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/ftc_ransomware_report_oct_2023.pdf. References herein to the 2023 Ransomware Report are for informational purposes and do not reflect current FTC leadership's endorsement of the 2023 Ransomware Report's views and conclusions.

[5] The Act refers in particular to the Russian Federation, the People's Republic of China (PRC), the Democratic People's Republic of Korea, and the Islamic Republic of Iran. The 2023 Ransomware Report and this report refer to these countries with the shorter names Russia, China or the PRC, North Korea, and Iran.

[6] The FTC has not engaged in foreign litigation regarding the topics identified in the RANSOMWARE Act.

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.[7] For this report, it is considered a subset of the broader category covered by the RANSOMWARE Act: cyber-related attacks. As explained in more detail in the introductory 2023 Ransomware Report, ransomware and cyber-related attacks arise most often in FTC matters related to data security and tech support scams.[8] The FTC plays a significant role in the overall effort by U.S. federal agencies to protect consumers and businesses against ransomware and other cyber-related attacks through its civil law enforcement tools in actions involving data security and tech support scams as well as through its guidance for consumer and business education.

A. The FTC's Data Security Program

Data security is an important FTC enforcement program requiring companies to take reasonable steps to safeguard consumer's personal data. Strong data security serves as a frontline defense against cyber attacks. Companies that collect, use, share, or transmit consumers' personal data must employ reasonable security measures, including encryption of sensitive information, to protect such information from unauthorized access, use, or disclosure.[9] The FTC's 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 maintain security and reduce vulnerabilities.[10] 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

---

[7] *See, e.g.,* FTC, Consumer Sentinel Network Subcategories, October 2024, Subcategory Name 52: Malware & Computer Exploits, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/CSNPSCFullDescriptions.pdf?utm_source=govdelivery ("[R]ansomware 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….").

[8] *See* 2023 Ransomware Report at 1-2; *see generally id.* Section I.

[9] FTC, Model Letter sent to Tech Companies from Chairman Ferguson (Aug. 21, 2025), *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/staff-letters/model-letter-sent-tech-companies-chairman-andrew-n-ferguson.

[10] *Cf.* Model Letter sent to Tech Companies from Chairman Andrew N. Ferguson (Aug. 21, 2025) *available at* https://www.ftc.gov/news-events/news/press-releases/2025/08/ftc-chairman-ferguson-warns-companies-against-censoring-or-weakening-data-security-americans-behest ("The Commission has steadfastly maintained that companies that collect, use, share, or transmit consumers' personal data must employ reasonable security measures, including encryption of sensitive information, to protect such information from unauthorized access, use, or disclosure"); Thomas B. Pahl, FTC, Stick with Security: Store sensitive personal information securely and protect it during transmission (Aug. 18, 2017), https://www.ftc.gov/business-guidance/blog/2017/08/stick-security-store-sensitive-personal-information-securely-protect-it-during-transmission; *Fed. Trade Comm'n v. Ring, LLC*, No. 23-cv-1549 (D.D.C. 2003) (alleging that failure to encrypt videos of consumers in private spaces of home, among other security failures, was unfair); *Chegg, Inc.*, Fed. Trade Comm'n No. 2023151 (2022) (same, as to personal information); *BJ's Wholesale Club, Inc.*, Fed. Trade Comm'n No. 0423160 (2005) (same, as to credit card information); 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.

not mean that a company violated the law.[11] This standard is the touchstone of the FTC's data security work involving data breaches, which very often involve a third-party cyber-related attack.[12] Faulty data security practices can also include a lack of training on how to handle spam such as phishing emails.[13]

To date, the FTC has brought more than 90 enforcement actions involving data security.[14] These actions have involved allegations that a company's security practices 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 injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition.[15] In many of these cases, although not all, the Commission alleged that the company's failure to reasonably 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.[16]

Furthermore, engaging in ransomware or some other cyber-related attack typically constitutes a criminal offense, and thus, as mentioned above, many U.S. criminal enforcement agencies also play a key role working on these challenges.[17] As a civil law enforcement agency, the Commission cannot itself 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 focus on company practices and their effects on protecting consumers' personal information. The FTC pursues these efforts regardless of the identity, location, and origin of the underlying malicious actor, as such threats can originate from anywhere in the world. The FTC also works in appropriate cases with federal agencies with criminal

---

[11] *See, e.g.,* 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.
[12] *See* 2023 Ransomware Report at 2.
[13] *See* FTC, Press Release, FTC Brings Action Against Ed Tech Provider Chegg for Careless Security that Exposed Personal Data of Millions of Customers (Oct. 31, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-brings-action-against-ed-tech-provider-chegg-careless-security-exposed-personal-data-millions.
[14] *See* FTC, Federal Trade Commission Testimony Before the Committee on Appropriations, Subcommittee On Financial Services And General Government, United States House Of Representatives (May 15, 2025) at 15, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-Chairman-Andrew-N-Ferguson-FSGG-Testimony-05-15-2025.pdf. *See generally* 2023 Ransomware Report at Section I.A. (providing historical examples of relevant FTC enforcement actions concerning data security).
[15] *See* 15 U.S.C. § 45(n).
[16] *See* FTC, Federal Trade Commission Testimony Before the Committee on Appropriations, Subcommittee On Financial Services And General Government, United States House Of Representatives (May 15, 2025) at 15, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-Chairman-Andrew-N-Ferguson-FSGG-Testimony-05-15-2025.pdf.
[17] *See, e.g.*, *supra* note 3; FBI, What We Investigate: Cyber Crime, https://www.fbi.gov/investigate/cyber (last accessed Dec. 10, 2025) (describing the FBI as "the lead federal agency for investigating cyberattacks and intrusions."); CISA, Cybersecurity and Infrastructure Security Agency: About CISA, https://www.cisa.gov/about (last accessed Dec. 10, 2025) (stating that CISA "lead[s] the national effort to understand, manage, and reduce the risk to cyber and physical infrastructure that Americans rely on every hour of every day" and serves "[a]s the National Coordinator for Critical Infrastructure Security and Resilience….").

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.[18]

The FTC also supports the criminal investigation and prosecution of identity theft by state and federal criminal law-enforcement agencies, which can result from a cyber attack, by serving as the federal clearinghouse for identity theft reports through its Consumer Sentinel Network database. As set forth in detail in the FTC 2023 SAFE WEB Report, the FTC has a robust system to collect, analyze, and report about consumer fraud complaints.[19] The genesis of FTC investigations and cases on data security, however, is rarely consumer complaints. One reason is that consumers are typically unaware of how a particular data breach or compromise of their personal data occurred. And, as explained further below, *infra* Section IV, consumers often do not file complaints, especially with the government. Instead, the FTC often learns about data breaches from the media or from the companies themselves and then may begin corresponding investigations.[20] 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.

In this reporting period, [21] the Commission continued enforcement actions against companies allegedly engaged in unreasonable data security practices that involved a cyber-related attack or breach. For example, the FTC pursued the following actions and settled all of them. In January 2025, the FTC brought an action against GoDaddy, one of the world's largest web hosting companies, for its failure to implement reasonable and appropriate security measures to protect and monitor its website-hosting environments for security threats, and misleading customers about the extent of its data security protections on its website hosting services.[22] According to the complaint, GoDaddy's data-security failures allegedly resulted in several major security breaches between 2019 and 2022, in which bad actors gained unauthorized access to GoDaddy's shared web hosting environment which contained

---

[18] *See generally* FTC, Criminal Liaison Unit, https://www.ftc.gov/enforcement/criminal-liaison-unit (last accessed Dec. 10, 2025).

[19] *See generally* 2023 SAFE WEB Report at Section I and Appendices A and B; FTC, Consumer Sentinel Network, www.sentinel.gov (last accessed Dec. 10, 2025).

[20] 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. *Cf.* 16 CFR Part 318, *available at* https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule.

[21] In addition to the matters from this reporting period that follow, just in December 2025 the Commission announced actions it took against alleged data security failures. *See* FTC, Press Release, FTC Will Require Illusory Systems to Return Money Stolen by Hackers and Implement an Information Security Program (Dec. 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/12/ftc-will-require-illusory-systems-return-money-stolen-hackers-implement-information-security-program ("The FTC is taking action against Illusory Systems Inc. for failing to implement adequate data security measures, leading to a major security breach in which hackers stole $186 million from consumers. Under a proposed order settling the FTC's allegations, Utah-based Illusory, which does business as Nomad, will be required to implement an information security program to address numerous alleged security failures and to return recovered money to affected consumers."); FTC, Press Release, FTC Takes Action Against Education Technology Provider for Failing to Secure Students' Personal Data (Dec. 1, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/12/ftc-takes-action-against-education-technology-provider-failing-secure-students-personal-data ("The FTC will require education technology provider Illuminate Education, Inc. (Illuminate) to implement a data security program and delete unnecessary data to settle allegations that the company's data security failures led to a major data breach, which allowed hackers to access the personal data of more than 10 million students.").

[22] FTC, Press Release, FTC Takes Action Against GoDaddy for Alleged Lax Data Security for Its Website Hosting Services (Jan. 15, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-takes-action-against-godaddy-alleged-lax-data-security-its-website-hosting-services.

customers' websites and associated consumer data related to these websites and underlying consumer transactions.[23] The FTC charged that these breaches allegedly resulted in harm to customers using GoDaddy to host their websites as well as to consumers visiting the websites, for example by compromising confidential information maintained in relation to the websites, redirecting consumers to malicious websites, and leaving consumers vulnerable to malware and malicious code that is likely to lead to ransomware attacks and identity theft.[24] The company allegedly failed, among other practices, to inventory and manage assets and software updates; assess risks to its shared hosting services; adequately log and monitor security-related events in the hosting environment; and fence off its shared hosting from less secure environments.[25] In addition, the company allegedly misled customers, through claims on its websites and in email and social media ads, by representing that it deployed reasonable security.[26] The FTC's final consent order, among other things, prohibits GoDaddy from making misrepresentations about its security and requires the company to establish and implement a comprehensive security program and to hire an independent third-party assessor to conduct reviews of the program.[27]

Additionally, in 2024, the Commission alleged that security camera firm Verkada failed to use appropriate information security practices, such as requiring unique and complex passwords, adequately encrypting customer data, and implementing secure network controls.[28] The complaint alleges that these failures resulted in at least two security breaches in 2020 and 2021, which allowed a hacker to access over 150,000 live Verkada customer cameras as well as other customer information like physical addresses, audio recordings, and customer WiFi credentials.[29] Through that access, the hacker allegedly viewed patients in psychiatric hospitals and women's health clinics as well as children playing inside a room.[30] The FTC further claimed that the company violated the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act in several ways, including by flooding prospective customers with a barrage of commercial emails and failing to include the option to unsubscribe or opt-out of those emails, honor opt-out requests, and provide a physical postal address in the emails.[31] Verkada subsequently entered a stipulated order with the FTC which required it to pay a $2.95 million penalty and to develop and implement a comprehensive information security program with third-party

---

[23] *See In the Matter of GoDaddy, Inc.*, Fed. Trade Comm'n 202-3133, Compl. ¶¶ 31-35, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/GoDaddy-Complaint.pdf.
[24] *See id.* ¶¶ 32-35.
[25] *See id.* ¶ 21; Press Release, FTC, FTC Takes Action Against GoDaddy for Alleged Lax Data Security for Its Website Hosting Services (Jan. 15, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-takes-action-against-godaddy-alleged-lax-data-security-its-website-hosting-services.
[26] *See In the Matter of GoDaddy, Inc.*, Fed. Trade Comm'n 202-3133, Compl. ¶¶ 37-38, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/GoDaddy-Complaint.pdf; FTC, Press Release, FTC Takes Action Against GoDaddy for Alleged Lax Data Security for Its Website Hosting Services (Jan. 15, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-takes-action-against-godaddy-alleged-lax-data-security-its-website-hosting-services.
[27] FTC, Press Release, FTC Finalizes Order with GoDaddy over Data Security Failures (May 21, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/05/ftc-finalizes-order-godaddy-over-data-security-failures; *see also In the Matter of GoDaddy, Inc.*, Fed. Trade Comm'n 202-3133, Decision and Order, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/GoDaddy-D%26O.pdf.
[28] FTC, Press Release, FTC Takes Action Against Security Camera Firm Verkada over Charges it Failed to Secure Videos, Other Personal Data and Violated CAN-SPAM Act (Aug. 30, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-takes-action-against-security-camera-firm-verkada-over-charges-it-failed-secure-videos-other.
[29] *See id.*; *United States v. Verkada, Inc.*, No. 24-cv-06153 (N.D. Cal. Aug. 30, 2024), ECF No. 1: Compl. ¶¶ 3, 21-30, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/2123068verkadacomplaint.pdf.
[30] *Id.* ¶ 27.
[31] *Id.*

audits, as well as prohibited it from making misrepresentations about its privacy and data security practices and from violating the CAN-SPAM Act.[32]

Similarly, in *Blackbaud*, the FTC in 2024 filed a complaint claiming that a company's lax security allowed a hacker to breach the company's network and access the personal data of millions of consumers, including Social Security and bank account numbers, and demand a ransom payment to prevent the hacker from exposing the stolen data.[33] The complaint alleged the following: Despite promising to customers that it took appropriate steps to safeguard consumer data, Blackbaud failed to put in place such safeguards, including monitoring hackers' attempts to breach its networks, segmenting data to prevent hackers from easily accessing its networks and databases, and adequately implementing multifactor authentication.[34] As a result of these failures, a hacker in 2020 accessed a customer's Blackbaud-hosted database then moved freely across multiple Blackbaud-hosted environments.[35] The breach then went undetected for three months, allowing the hacker to remove massive amounts of unencrypted consumer data belonging to Blackbaud's customers.[36] Once it detected the breach, the company agreed to pay the hacker a ransom of 24 Bitcoin, worth about $250,000, after the hacker threatened to expose the stolen data; but the company never verified that the hacker actually deleted the stolen data.[37] Blackbaud waited nearly two months after that to notify its customers about the breach and then misled consumers about the extent their data that was stolen, telling customers they did not need to take any action in response to the breach.[38] This delay harmed consumers who were unable to take steps

---

[32] *See id.*; *see also United States v. Verkada, Inc.*, No. 24-cv-06153 (N.D. Cal. Aug. 30, 2024), ECF No. 6: Stip. Order, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/2123068verkadasignedorder.pdf.
[33] FTC, Press Release, FTC Order Will Require Blackbaud to Delete Unnecessary Data, Boost Safeguards to Settle Charges its Lax Security Practices Led to Data Breach (Feb. 1, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-require-blackbaud-delete-unnecessary-data-boost-safeguards-settle-charges-its-lax.
[34] *See id.*; *see also In the Matter of Blackbaud, Inc.*, Fed Trade Comm'n 2023181, Compl. ¶ 19, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Blackbaud-Complaint.pdf.
[35] *See* FTC, Press Release, FTC Order Will Require Blackbaud to Delete Unnecessary Data, Boost Safeguards to Settle Charges its Lax Security Practices Led to Data Breach (Feb. 1, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-require-blackbaud-delete-unnecessary-data-boost-safeguards-settle-charges-its-lax; *see also In the Matter of Blackbaud, Inc.*, Fed Trade Comm'n 2023181, Compl. ¶¶ 6-10, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Blackbaud-Complaint.pdf.
[36] *See* FTC, Press Release, FTC Order Will Require Blackbaud to Delete Unnecessary Data, Boost Safeguards to Settle Charges its Lax Security Practices Led to Data Breach (Feb. 1, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-require-blackbaud-delete-unnecessary-data-boost-safeguards-settle-charges-its-lax; *see also In the Matter of Blackbaud, Inc.*, Fed Trade Comm'n 2023181, Compl. ¶¶ 6-10, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Blackbaud-Complaint.pdf.
[37] *See* FTC, Press Release, FTC Order Will Require Blackbaud to Delete Unnecessary Data, Boost Safeguards to Settle Charges its Lax Security Practices Led to Data Breach (Feb. 1, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-require-blackbaud-delete-unnecessary-data-boost-safeguards-settle-charges-its-lax; *see also In the Matter of Blackbaud, Inc.*, Fed Trade Comm'n 2023181, Compl. ¶ 11, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Blackbaud-Complaint.pdf.
[38] *See* FTC, Press Release, FTC Order Will Require Blackbaud to Delete Unnecessary Data, Boost Safeguards to Settle Charges its Lax Security Practices Led to Data Breach (Feb. 1, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-require-blackbaud-delete-unnecessary-data-boost-safeguards-settle-charges-its-lax; *see also In the Matter of Blackbaud, Inc.*, Fed Trade Comm'n 2023181, Compl. ¶¶ 12-16, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Blackbaud-Complaint.pdf.

to protect themselves from potential identity theft and other potential harms resulting from the breach.[39] As part of a settlement, Blackbaud is prohibited from misrepresenting its data security and data retention policies, and was required to delete data that it no longer needs to provide its products or services; develop a comprehensive information security program that addresses the issues highlighted by the FTC's complaint; implement a data retention schedule outlining its data deletion practices; and notify the FTC if it experiences a future data breach that it is required to report to any other local, state, or federal agency.[40]

In November 2023, the Commission took action against Global Tel*Link, claiming that the company and two of its subsidiaries failed to implement adequate security safeguards to protect personal information they collect from users of its services, which enabled bad actors to gain access to unencrypted personal information stored in the cloud and used for testing.[41] According to the FTC, in August 2020, as a result of changes made by the company's third-party vendor to the security settings for the data stored in the cloud, the personal data of many Global Tel*Link customers was left accessible via the internet without any safeguards to prevent unauthorized people from accessing and removing data from the test site until a security researcher alerted the company about the security holes.[42] A forensic analysis showed that hackers accessed billions of bytes of the exposed data, including personally identifiable information and payment card numbers, financial account information, and Social Security numbers.[43] The complaint alleged that Global Tel*Link was subsequently notified by an identity monitoring company that personal data belonging to Global Tel*Link customers was available on the dark web, but Global Tel*Link waited approximately nine months to notify affected customers that their personal data may have been compromised as a result of the data breach.[44] It also allegedly contacted only 45,000 customers as part of that effort, despite the breach having possibly affected hundreds of thousands of additional customers.[45] This nine-month delay, according to the complaint, further harmed customers who did not have an opportunity to take actions to protect themselves from identity theft by implementing a credit freeze or other measures.[46] The FTC further alleged that the

---

[39] *See* FTC, Press Release, FTC Order Will Require Blackbaud to Delete Unnecessary Data, Boost Safeguards to Settle Charges its Lax Security Practices Led to Data Breach (Feb. 1, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-require-blackbaud-delete-unnecessary-data-boost-safeguards-settle-charges-its-lax; *see also In the Matter of Blackbaud, Inc.*, Fed Trade Comm'n 2023181, Compl. ¶¶ 12-16, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Blackbaud-Complaint.pdf.

[40] *See* FTC, Press Release, FTC Finalizes Order with Blackbaud Related to Allegations the Firm's Security Failures Led to Data Breach (May 20, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/05/ftc-finalizes-order-blackbaud-related-allegations-firms-security-failures-led-data-breach; *see also In the Matter of Blackbaud, Inc.*, Fed Trade Comm'n 2023181, Decision, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/2023181_blackbaud_final_consent_package.pdf.

[41] *See* FTC, Press Release, FTC Takes Action Against Global Tel*Link Corp. for Failing to Adequately Secure Data, Notify Consumers After Their Personal Data Was Breached (Nov. 16, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/11/ftc-takes-action-against-global-tellink-corp-failing-adequately-secure-data-notify-consumers-after.

[42] *See id.*; *see also In the Matter of Global Tel*Link Corporation et al.*, Fed Trade Comm'n 2123012, Compl. ¶¶ 29-37, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Complaint-GlobalTelLinkCorp.pdf

[43] *See* FTC, Press Release, FTC Takes Action Against Global Tel*Link Corp. for Failing to Adequately Secure Data, Notify Consumers After Their Personal Data Was Breached (Nov. 16, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/11/ftc-takes-action-against-global-tellink-corp-failing-adequately-secure-data-notify-consumers-after.

[44] *See id.*

[45] *See id.*

[46] *See id.*; *see also In the Matter of Global Tel*Link Corporation et al.*, Fed Trade Comm'n 2123012, Compl. ¶ 41, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Complaint-GlobalTelLinkCorp.pdf.

company repeatedly and falsely claimed in marketing materials following the incident that it had never suffered a data breach.[47] As part of a settlement, Global Tel*Link and its two subsidiaries are prohibited from misrepresenting their data security practices and will be required to implement a comprehensive data security program; notify users affected by the data breach who did not previously receive notice and provide them with credit monitoring and identity protection products; and notify users of future security incidents that trigger any federal, state, or local breach reporting requirements.[48]

While the Commission may sometimes obtain information about the sources of hacks involved in its data security cases, as a civil law enforcement agency, the typical focus of the FTC's investigations and legal actions is on the companies' practices rather than pursuing action against the malicious actors involved.

Nevertheless, relevant to this Report, the Commission has, on a number of occasions, received information suggesting that malicious actors involved in data breaches were located in China or Russia.[49] The agency is aware of public reports that large Chinese companies often have ties to the Chinese Communist Party (CCP).[50] Moreover, the agency is aware of other potential connections to the government of the People's Republic of China (PRC) in the context of data security breaches, such as

---

[47] *See* FTC, Press Release, FTC Takes Action Against Global Tel*Link Corp. for Failing to Adequately Secure Data, Notify Consumers After Their Personal Data Was Breached (Nov. 16, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/11/ftc-takes-action-against-global-tellink-corp-failing-adequately-secure-data-notify-consumers-after; *see also In the Matter of Global Tel*Link Corporation et al.*, Fed Trade Comm'n 2123012, Compl. ¶¶ 38-44, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Complaint-GlobalTelLinkCorp.pdf.

[48] *See* FTC, Press Release, FTC Finalizes Order with Global Tel*Link Over Security Failures that Led to Breach of Sensitive Data (Feb. 23, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-finalizes-order-global-tellink-over-security-failures-led-breach-sensitive-data; *see also In the Matter of Global Tel*Link Corporation et al.*, Fed Trade Comm'n 2123012, Decision and Order, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/D%26OGlobalTelLink.pdf.

[49] *See generally* 2023 Ransomware Report at 5-6 (providing historical examples of data security breach cases involving connections to China and Russia).

[50] *See, e.g.*, Code of Corporate Governance for Listed Companies, Art. 5, China Securities Regulatory Commission, *available at* http://www.csrc.gov.cn/csrc_en/c102034/c1372459/1372459/files/P020190415336431477120.pdf (last accessed Dec. 10, 2025) (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."); Jeffrey Becker, Center for Naval Analyses (CAN), Fused Together: The Chinese Communist Party Moves Inside China's Private Sector (September 6, 2024), https://www.cna.org/our-media/indepth/2024/09/fused-together-the-chinese-communist-party-moves-inside-chinas-private-sector ("[T]he Chinese Communist Party (CCP) has methodically pursued a policy of expanded control and oversight of the private sector. Today, the party has a much greater ability to monitor and influence the decision-making of private Chinese firms."); 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.").

the DOJ's 2020 prosecution of four members of PRC's military for a hack of Equifax,[51] which the Director of National Intelligence attributed to the PRC government or cyber actors based in the PRC.[52]

In this reporting period, the FTC brought an action in 2024 against Marriott International, Inc. and its subsidiary Starwood Hotels & Resorts Worldwide LLC. The FTC alleged that, between 2014 and 2020, the companies' security failures resulted in three large data breaches—the second of which news outlets and other federal agencies attributed to malicious actors connected to the PRC government[53]—that exposed information about more than 344 million customers worldwide.[54] During that same time, Marriott and Starwood also allegedly deceived consumers by claiming to have reasonable and appropriate data security.[55] Notwithstanding these claims, the FTC's complaint provided, the companies failed to deploy reasonable or appropriate security to protect personal information, including implementing appropriate password, access, and firewall controls as well as patching outdated software and systems, adequately logging and monitoring network requirements, and deploying adequate multifactor authentication.[56]

The first data breach in that matter allegedly began in June 2014 and involved the payment card information of more than 40,000 Starwood customers, and it went undetected for 14 months until Starwood notified customers in November 2015, four days after Marriott announced it was acquiring Starwood.[57] The second breach allegedly began around July 2014 and went undetected until September 2018, and it involved malicious actors that accessed 339 million Starwood guest account records

---

[51] *See* U.S. Department of Justice, Press Release, Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax, Remarks as Prepared for Delivery (Feb. 10, 2020), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military; *see generally* 2023 Ransomware Report at 6.

[52] *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.

[53] *See, e.g.,* 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 ("Recent breaches attributed to the PRC government or to cyber actors based in China include … the theft from Marriott hotels of roughly 400 million records."); U.S. Department of Justice, Press Release, 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 ("For years, we have witnessed China's voracious appetite for the personal data of Americans, including … the intrusion into Marriott hotels."); David E. Sanger, New York Times, Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing (Dec. 11, 2018), https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html.

[54] *See* FTC, Press Release, FTC Takes Action Against Marriott and Starwood Over Multiple Data Breaches (Oct. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-takes-action-against-marriott-starwood-over-multiple-data-breaches.

[55] *See* FTC, Press Release, FTC Takes Action Against Marriott and Starwood Over Multiple Data Breaches (Oct. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-takes-action-against-marriott-starwood-over-multiple-data-breaches.

[56] *Id.*

[57] *Id.*; *see also In the Matter of Marriott International, Inc.*, Fed Trade Comm'n 1923022, Compl. ¶¶ 8-10, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/1923022marriottcomplaint.pdf.

worldwide, including 5.25 million unencrypted passport numbers.[58] The third breach, which allegedly went undetected from September 2018 until February 2020, impacted Marriott's network and involved malicious actors' access to 5.2 million guest records containing personal information.[59] As part of a settlement, Marriott is required to implement a comprehensive information security program to help safeguard customers' personal information; implement a policy to retain personal information only for as long is reasonably necessary; establish a link on their website for U.S. customers to request for personal information associated with their email address or loyalty rewards account number to be deleted; and review loyalty rewards accounts upon customer request and restore stolen loyalty points.[60]

In sum, 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 complements these efforts and serves as a first line of defense against those attacks.

B. Tech Support Scams

The Commission also plays an important role in the fight against "tech support" scams, which are a frequent form of imposter scams and similar to ransomware.[61] In these scams, individuals connect with people through computer pop-up warnings, phone calls, or online ads or websites appearing in search results for tech support help. Those scammers then trick people into paying for unnecessary tech support services or to fix a nonexistent problem. Scammers sometimes pretend to be from a well-known tech company and convince consumers that there are problems with their computers. They 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." Once in contact with consumers, the scammers will then employ a litany of tactics, including asking consumers for remote access to their computers to access information, enrolling consumers in worthless maintenance or warranty programs, and/or obtaining credit card information to bill consumers for worthless services. In some instances, the scammers will misrepresent that the consumers' computers have already been

[58] FTC, Press Release, FTC Takes Action Against Marriott and Starwood Over Multiple Data Breaches (Oct. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-takes-action-against-marriott-starwood-over-multiple-data-breaches; *see also In the Matter of Marriott International, Inc.*, Fed Trade Comm'n 1923022, Compl. ¶¶ 11-16, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/1923022marriottcomplaint.pdf.

[59] FTC, Press Release, FTC Takes Action Against Marriott and Starwood Over Multiple Data Breaches (Oct. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-takes-action-against-marriott-starwood-over-multiple-data-breaches; *see also In the Matter of Marriott International, Inc.*, Fed Trade Comm'n 1923022, Compl. ¶¶ 17-21, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/1923022marriottcomplaint.pdf.

[60] FTC, Press Release, FTC Finalizes Order with Marriott and Starwood Requiring Them to Implement a Robust Data Security Program to Address Security Failures (Dec. 20, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-finalizes-order-marriott-starwood-requiring-them-implement-robust-data-security-program-address; *see also In the Matter of Marriott International, Inc.*, Fed Trade Comm'n 1923022, Decision and Order, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/1923022marriottfinalorder.pdf.

[61] *See generally* 2023 Ransomware Report at Section I.B.

infected with malicious software (or "malware"), such as a virus or spyware,[62] or install malware that gives the scammers access to sensitive data.[63]

The FTC has taken action against perpetrators of tech support fraud, including by cooperating with foreign counterparts to stop scammers harming American consumers from abroad.[64] In this reporting period, the FTC in *Restoro-Reimage* sued Cyprus-based companies Restoro Cyprus Limited and Reimage Cyprus Limited, claiming that they bilked tens of millions of dollars from consumers, particularly older consumers, by duping them into buying computer repair services.[65] Consumers were, for example, allegedly lured or alarmed by fake Microsoft Windows pop-ups, which stated that their computer or system was infected with viruses and which urged them to "scan" their computers "To avoid more damage."[66] The FTC alleged that regardless of the actual health of the consumers' computers, the companies' scans typically identified purported serious issues that needed immediate attention.[67] Following the scans, the companies allegedly urged consumers to purchase their software online to "fix" the alleged problems or remove alleged viruses and malware.[68] Furthermore, according to the complaint, when consumers would call a number provided by the companies to "activate" the software, telemarketers would subsequently attempt to sell additional services by accessing consumers' computers and misrepresenting that routine computer errors and messages were signs of malware, viruses, or other problems. Moreover, the FTC alleged those telemarketers routinely claimed that the "problems" on consumers' computers could not be fixed with the newly purchased software alone and required help from a Restoro or Reimage technician, which cost hundreds of dollars more.[69] As part of a settlement, the companies are required to pay $26 million to provide redress to affected consumers, and are prohibited from misrepresenting security or performance issues or any other material issues related to the sale, marketing or distribution of any product or service and from engaging in deceptive

[62] *Cf.* FTC, Combatting Spyware and Malware, https://www.ftc.gov/news-events/topics/identity-theft/spyware-malware (last accessed Dec. 10, 2025).
[63] *See, e.g.,* FTC, Cybersecurity for Small Business, Tech Support Scams (Sept. 2025), https://www.ftc.gov/business-guidance/small-businesses/cybersecurity; FTC, Press Release, FTC Obtains Settlements from Operators of Tech Support Scams (Oct. 26, 2017), https://www.ftc.gov/news-events/news/press-releases/2017/10/ftc-obtains-settlements-operators-tech-support-scams.
[64] *See* 2023 Ransomware Report at Section I.B (providing historical examples of the FTC's enforcement actions against tech support scams). Since 2012, the FTC has initiated law enforcement actions against at least 116 defendants associated with tech support scams.
[65] *See* FTC, Press Release, Tech Support Firms Will Pay $26 Million to Settle FTC Charges That They Deceived Consumers into Buying Repair Services (Mar. 14, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/03/tech-support-firms-will-pay-26-million-settle-ftc-charges-they-deceived-consumers-buying-repair; *see also Fed. Trade Comm'n v. Restoro Cyprus Limited, et al.*, No. 24-cv-00735 (D.D.C. Mar. 14, 2024), ECF No. 1:, Compl. ¶¶ 10-50, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/1-ComplaintagainstRestoro.pdf.
[66] FTC, Press Release, Tech Support Firms Will Pay $26 Million to Settle FTC Charges That They Deceived Consumers into Buying Repair Services (Mar. 14, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/03/tech-support-firms-will-pay-26-million-settle-ftc-charges-they-deceived-consumers-buying-repair.
[67] *Id.*
[68] *Id.*
[69] *Id.*

telemarketing.[70] In March 2025, the FTC announced that it was sending redress payments to affected consumers.[71]

In addition, the FTC has pursued those who assist and facilitate such frauds or other cyber-related attacks.[72] In this reporting period, the FTC settled allegations against Walmart, which claimed that the company processed fraudulent money transfers related to cyber or malware scams.[73] As part of the settlement, the company agreed to pay a $10 million judgment and is prohibited from providing money transfer services without taking timely and appropriate action to effectively detect and prevent fraud-induced money transfers, among other requirements.[74] The same month the parties settled in *Walmart*, the FTC brought a lawsuit against payment processor Paddle.com Market Limited and its subsidiary, Paddle.com, Inc., claiming that Paddle abused the U.S. credit-card system and processed payments for tech-support telemarketers.[75] Paddle agreed to pay $5 million for consumer redress and is, among other requirements, prohibited from processing payments for tech-support merchants that engage in telemarketing.[76] Taken together, these enforcement actions constitute important domestic and cross-border work to stop tech support scams and the harm they inflict on American consumers.

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. In this reporting period, the FTC continued to build upon its consumer and business education efforts, providing dynamic guidance to consumers and businesses, including tools that they can use to protect themselves against such threats.[77] The FTC has also worked across government and beyond to raise awareness about these important issues.

---

[70] *Id.*; *see also Fed. Trade Comm'n v. Restoro Cyprus Limited, et al.*, No. 24-cv-00735 (D.D.C. Mar. 14, 2024), ECF No. 6:, Stip. Order, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Restoro.SignedOrder.pdf.
[71] *See* FTC, Press Release, FTC Sends More than $25.5 Million to Consumers Impacted by Tech Support Firms' Scam (Mar. 10, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/03/ftc-sends-more-255-million-consumers-impacted-tech-support-firms-scam.
[72] *See* 2023 Ransomware Report at 9 (providing historical examples of FTC actions against facilitators of tech support scams).
[73] *See* FTC, Press Release, Walmart to Pay $10 Million to Settle FTC Allegations it Allowed Scammers to Obtain Millions from Consumers Using Company's Wire Transfer Services (June 20, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/06/walmart-pay-10-million-settle-ftc-allegations-it-allowed-scammers-obtain-millions-consumers-using.
[74] *See id.*
[75] *See* FTC, Press Release, Paddle Will Pay $5 Million to Settle FTC Allegations of Unfair Payment-Processing Practices and Facilitation of Deceptive Tech-Support Schemes (June 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/06/paddle-will-pay-5-million-settle-ftc-allegations-unfair-payment-processing-practices-facilitation.
[76] *See id.*
[77] *See generally* 2023 Ransomware Report at Section I.C. (providing additional historical examples of the FTC's public education and guidance on cybersecurity, ransomware, and other cyber-related attacks).

Specifically, the FTC's consumer and business education efforts include up-to-date alerts and advice about malware,[78] cybersecurity,[79] and tech support scams.[80] FTC staff has issued consumer alerts on protecting devices from cryptojacking,[81] malware from illegal video streaming apps,[82] what to do about email hacks,[83] phishing,[84] and scams related to cloud storage.[85] The FTC has also published articles and blogs for consumers on how to protect themselves and their personal information from scammers[86] as well as from malware[87] and phishing.[88] Similarly, the FTC has issued consumer alerts and published articles and infographics that address various tech support scam issues. These have included advice on how to spot, avoid, and report tech support scams (*see infra*, *Photo 1*),[89] counseling consumers not to pay when someone demands a gift card or wire transfer through a service like MoneyGram or Western Union,[90] and how to spot tech scammers who claim that a third party hacked into a consumer's financial account (*see infra*, *Photo 2*),[91] as well as how to avoid "free" computer security scans[92] and scams

[78] *See* FTC, Malware: How to Protect Against, Detect, and Remove It (Apr. 2025), https://consumer.ftc.gov/articles/malware-how-protect-against-detect-and-remove-it.
[79] *See,* FTC, Cybersecurity for Small Business (Sept. 2025), https://www.ftc.gov/business-guidance/small-businesses/cybersecurity.
[80] *See id.*
[81] *See* Jason Adler, FTC, Protecting your devices from cryptojacking (June 23, 2022), https://consumer.ftc.gov/consumer-alerts/2022/06/protecting-your-devices-cryptojacking.
[82] *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.
[83] *See* FTC, Hacked Email: What to Do, https://www.ftc.gov/media/video-0104-hacked-email-what-do (last accessed Jan 15, 2026).
[84] *See* Ari Lazarus, FTC, Phishing scams can be hard to spot (Dec. 11, 2024), https://consumer.ftc.gov/consumer-alerts/2024/12/phishing-scams-can-be-hard-spot; Ari Lazarus, FTC, Scammers are delivering phishing messages this holiday season (Dec. 2, 2024), https://consumer.ftc.gov/consumer-alerts/2024/12/scammers-are-delivering-phishing-messages-holiday-season; Alexandra House, FTC, Don't take the bait on phishing scams (Sept. 4, 2024), https://consumer.ftc.gov/consumer-alerts/2024/09/dont-take-bait-phishing-scams.
[85] *See* FTC, Are you really out of Cloud storage or is that message a scam? (July 2, 2025), https://consumer.ftc.gov/consumer-alerts/2025/07/are-you-really-out-cloud-storage-or-message-scam.
[86] *See* FTC, Protect Your Personal Information From Hackers and Scammers (Nov. 2024), https://consumer.ftc.gov/articles/protect-your-personal-information-hackers-and-scammers; FTC, Alvaro Puig, Five ways to keep scammers and hackers away (Aug. 23, 2024), https://consumer.ftc.gov/consumer-alerts/2024/08/five-ways-keep-scammers-hackers-away.
[87] *See* FTC, Malware: How to Protect Against, Detect, and Remove It (Apr. 2025), https://consumer.ftc.gov/articles/malware-how-protect-against-detect-and-remove-it; FTC, Protecting Your Computer From Malware, https://consumer.ftc.gov/media/79889 (last accessed Jan. 15, 2025).
[88]FTC, How to Recognize and Avoid Phishing Scams (Sept. 2022), https://consumer.ftc.gov/articles/how-recognize-avoid-phishing-scams.
[89] *See* FTC, Infographic: How to Spot a Tech Support Scam, https://consumer.ftc.gov/sites/default/files/articles/pdf/tech-support-scam-infographic-508-v3.pdf (last accessed Jan. 15, 2026); *see also* FTC, How To Spot, Avoid, and Report Tech Support Scams (Sept. 2025), https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams; FTC, Tech Support Imposter Scams, https://consumer.ftc.gov/media/79958 (last accessed Dec. 10, 2025).
[90] *See* Cristina Miranda, FTC, No gift cards for tech support scammers (June 23, 2022), https://consumer.ftc.gov/consumer-alerts/2018/06/no-gift-cards-tech-support-scammers.
[91] *See* Amy Hebert, FTC, New tech support scammers want your life savings (Mar. 7, 2024), https://consumer.ftc.gov/consumer-alerts/2024/03/new-tech-support-scammers-want-your-life-savings.
[92] *See* Gema de las Heras, FTC, What to know before you click on a "free" computer security scan (Mar. 14, 2024), https://consumer.ftc.gov/consumer-alerts/2024/03/what-know-you-click-free-computer-security-scan.

involving seemingly urgent security messages.[93]

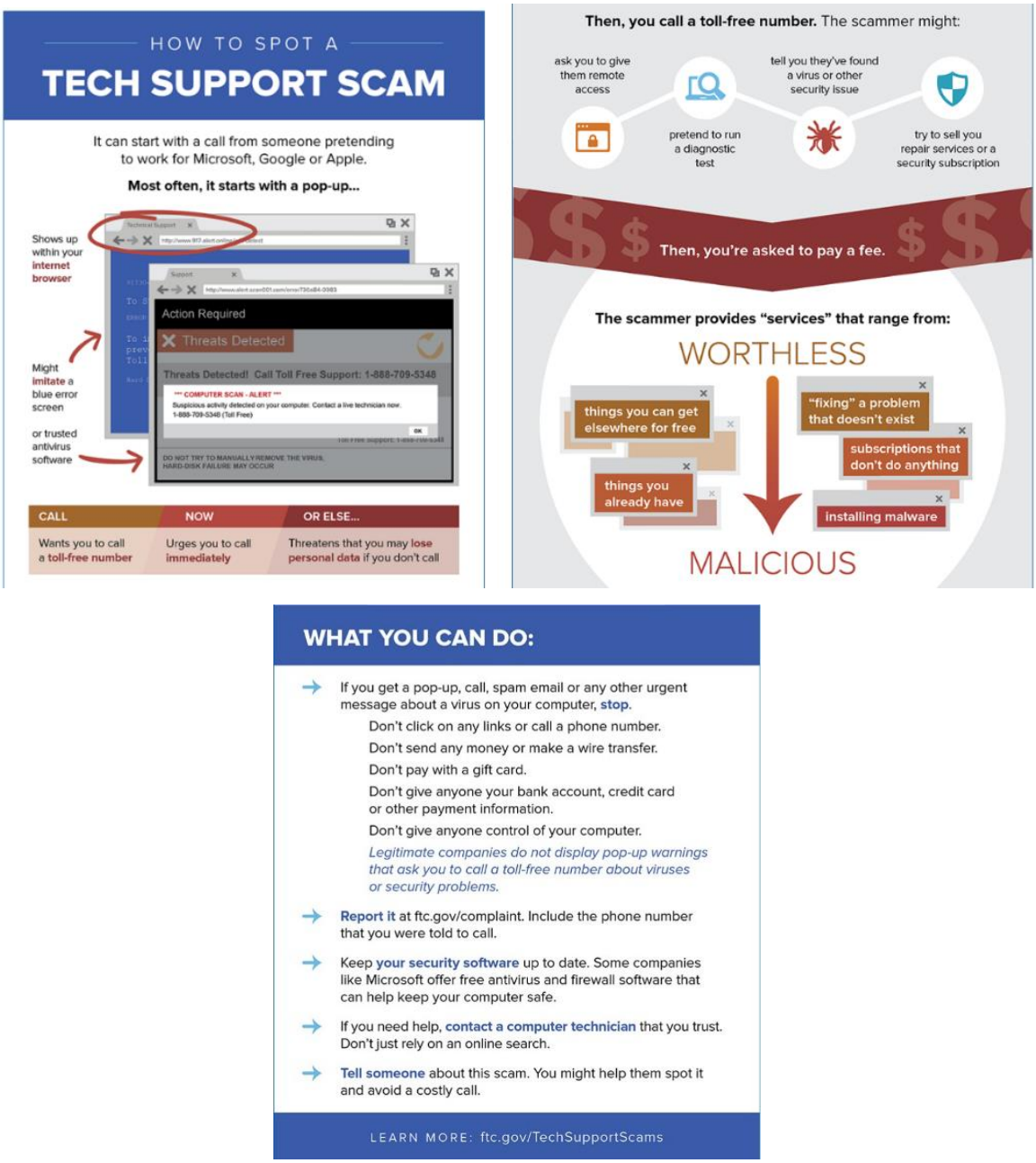


Photo 1 (Infographic on how to spot a tech support scam)

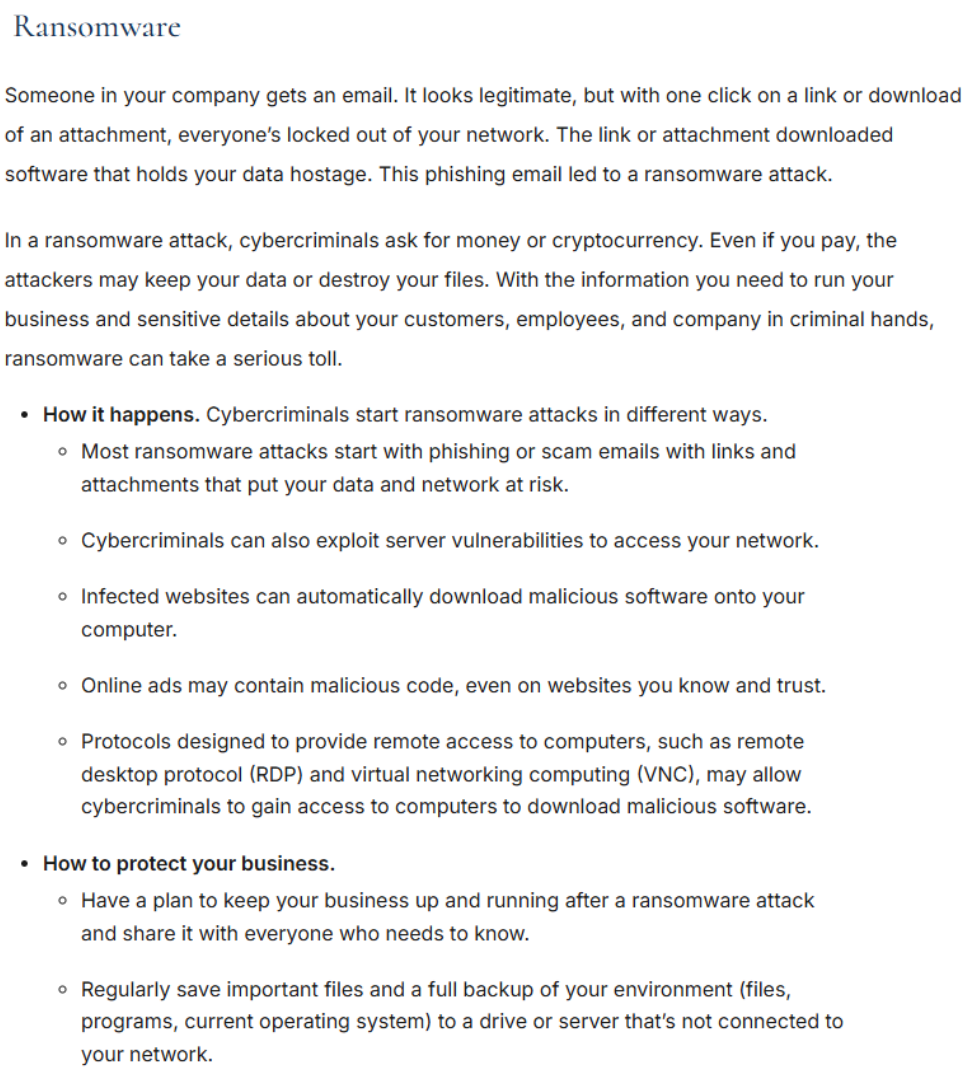
[93] *See* FTC, Seemingly urgent security messages could lead to tech support scams (Apr. 14, 2025), https://consumer.ftc.gov/consumer-alerts/2025/04/seemingly-urgent-security-messages-could-lead-tech-support-scams.

Photo 2 (Infographic on avoiding scammers that try to steal consumers' life savings)

The FTC's business education program provides guidance on cybersecurity, including information on ransomware, other cyber-related attacks, and tech support scams, as well. This business education may be particularly helpful for small businesses as a starting place to 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 have more educated conversations on those topics with their employees, vendors, and others about cybersecurity.[94] These materials include a central and easily accessible website that covers a range of cybersecurity topics such as ransomware (*see infra*, *Photo 3*),[95] tech support scams,[96] and other cyber-related attacks. The FTC's business guidance efforts also include

[94] *See, e.g.,* FTC, Cybersecurity for Small Businesses (Sept. 2025), https://www.ftc.gov/business-guidance/small-businesses/cybersecurity; FTC, Data Security, https://www.ftc.gov/business-guidance/privacy-security/data-security (last accessed Jan. 15, 2026); FTC, Start with Security: A guide for Business (August 2023), https://www.ftc.gov/business-guidance/resources/start-security-guide-business.
[95] *See* FTC, Cybersecurity for Small Business (Sept. 2025), https://www.ftc.gov/business-guidance/small-businesses/cybersecurity#common_cyberattacks.
[96] *See id.*

blogs on ransomware prevention,[97] a video on defending against and responding to ransomware,[98] and even a quiz to test businesses' knowledge on ransomware.[99]



Ransomware

Someone in your company gets an email. It looks legitimate, but with one click on a link or download of an attachment, everyone's locked out of your network. The link or attachment downloaded software that holds your data hostage. This phishing email led to a ransomware attack.

In a ransomware attack, cybercriminals ask for money or cryptocurrency. Even if you pay, the attackers may keep your data or destroy your files. With the information you need to run your business and sensitive details about your customers, employees, and company in criminal hands, ransomware can take a serious toll.

- **How it happens.** Cybercriminals start ransomware attacks in different ways.
  - Most ransomware attacks start with phishing or scam emails with links and attachments that put your data and network at risk.
  - Cybercriminals can also exploit server vulnerabilities to access your network.
  - Infected websites can automatically download malicious software onto your computer.
  - Online ads may contain malicious code, even on websites you know and trust.
  - Protocols designed to provide remote access to computers, such as remote desktop protocol (RDP) and virtual networking computing (VNC), may allow cybercriminals to gain access to computers to download malicious software.
- **How to protect your business.**
  - Have a plan to keep your business up and running after a ransomware attack and share it with everyone who needs to know.
  - Regularly save important files and a full backup of your environment (files, programs, current operating system) to a drive or server that's not connected to your network.

Photo 3 (FTC webpage providing resources for small business on cybersecurity, including ransomware)

Furthermore, the FTC has informed and brought together key players on these topics through public outreach. To leverage a wide range of expertise, the FTC has, for example, cooperated with other key

[97] *See* Lesley 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 Rossen, FTC, Ransomware prevention: An update for businesses (Dec. 11, 2020), https://www.ftc.gov/business-guidance/blog/2020/12/ransomware-prevention-update-businesses.
[98] *See* Youtube, Ransomware - Cybersecurity for Small Business | Federal Trade Commission, https://www.youtube.com/watch?v=cy2ZWi49E2A (last accessed Jan. 15, 2026).
[99] *See* FTC, Ransomware Quiz, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/quiz/ransomware (last accessed Jan. 15, 2026).

federal agencies, such as the National Institute of Standards and Technology (NIST), the Department of Homeland Security, and the Small Business Administration (SBA). In this reporting period, FTC staff continued its collaboration with the SBA, addressing cybersecurity and other resources for small businesses in a webinar and during SBA's National Small Business Week virtual summit, as well as discussing possible closer collaboration to protect consumers and businesses. FTC staff similarly continued its cooperation with NIST, exploring possibilities for joint public outreach and presentations. FTC staff also engaged in other forms of outreach including, for example, speaking with employees of Lowe's Home Improvement Centers about business email compromise, imposter scams, ransomware, and other types of fraud that target businesses of any size. And FTC staff presented information to local law enforcement authorities on common scams targeting small businesses and protective practices to keep information secure.

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 but likely connections to China and Russia. As explained further in the 2023 Ransomware Report,[100] these connections may include 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 appeared most often in enforcement actions concerning violations of consumer privacy and data 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, as mentioned above, the FTC takes enforcement action when companies misrepresent to consumers that they will not share their personal information and then do so, or when companies share consumers' personal information in ways that cause or are likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition.[101] In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices in or affecting commerce.[102] 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 (COPPA), Fair Credit Reporting Act, Gramm-Leach-Bliley Act, and Health Breach Notification Rule.[103] Furthermore, the Protecting Americans' Data from Foreign Adversaries Act

[100] *See* 2023 Ransomware Report at Section II.
[101] *See* 15 U.S.C. § 45(n).
[102] *See* 15 U.S.C. § 45.
[103] *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 Dec. 10, 2025).

(PADFAA)[104] enables the FTC to take action against businesses that sell, license, transfer, disclose, or provide access to Americans' sensitive personal data that the businesses did not collect to foreign adversary countries or any entity that is controlled by a foreign adversary country.[105] "Foreign adversary country" under PADFAA is defined by statute and currently includes China, Iran, North Korea, and Russia.[106]

Some of the Commission's enforcement actions concerning privacy and data security have involved parties with connections to China.[107] In this reporting period, the Commission continued to encounter connections to China in its privacy and data security enforcement actions.[108]

In *TikTok*, for example, the Commission alleged that video-sharing platform TikTok, its parent company at the time ByteDance,[109] and its affiliated companies violated COPPA and an existing 2019 stipulated FTC order against TikTok's predecessor companies for prior COPPA violations.[110] According to the

---

[104] PADFAA, Pub. Law No.118-50(I) (Apr. 24, 2024), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/padfa_plaw-118-50.pdf.

[105] *See e.g.,* FTC, Protecting Americans' Data from Foreign Adversaries Act of 2024 ("PADFAA"), https://www.ftc.gov/legal-library/browse/statutes/protecting-americans-data-foreign-adversaries-act-2024-padfaa (last accessed Dec. 10, 2025); Remarks of Commissioner Melissa Holyoak at IAPP Global Privacy Summit 2025: Privacy Enforcement Priorities for the Digital Economy (Apr. 22, 2025) at 6, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/holyoak-remarks-2025-iapp-global-privacy-summit.pdf. The Department of Justice enforces a rule that similarly restricts the transfer of American's sensitive personal data to countries of concern. *See id.* ("[I]n the future there may be opportunities to partner with the Department of Justice, as it enforces its recently enacted rule that restricts the transfer of Americans' sensitive personal data to countries of concern." (citing Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 28 C.F.R § 202 (2025)).

[106] *See* PADFAA, Section 2(c)(4) ("The term 'foreign adversary country' means a country specified in section 4872(d)(2) of title 10, Untied States Code."); 10 U.S.C. § 4872(d)(2) ("The term 'covered nation' means … the Democratic People's Republic of North Korea; … the People's Republic of China; … the Russian Federation; … [and] the Islamic Republic of Iran.").

[107] *See* 2023 Ransomware Report at Section II.A. (providing historical examples of FTC privacy and data security enforcement actions involving connections to China).

[108] In addition to the cases referred to in this Report, the Commission in September 2025 recently took action against robot toy maker Apitor Technology over allegations that its app enabled a third party in China to collect geolocation information from children without parental consent. *See* FTC, Press Release, FTC Takes Action Against Robot Toy Maker for Allowing Collection of Children's Data without Parental Consent (Sept. 3, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-takes-action-against-robot-toy-maker-allowing-collection-childrens-data-without-parental-consent; The complaint alleges that despite claims in Apitor's privacy policies that it complies with Children's Online Privacy Protection Rule (COPPA Rule), Apitor failed to notify parents and obtain their consent before collecting, or causing a third party to collect, geolocation data from children as required by COPPA. As part of a proposed order to settle the allegations, the company will be required to, among other things, ensure that ensure that any third-party software it uses is in compliance with the COPPA Rule and pay a $500,000 penalty.

[109] At the time, TikTok was owned and operated by the Chinese parent company ByteDance. It has since been the subject of a deal through which a new American entity would own and operate the company. *See TikTok finalizes a deal to form a new American entity*, APNews (Jan. 23, 2025), https://apnews.com/article/tiktok-deal-us-china-eccb46c3bfee4cf3d362a01fe4968a4f.

[110] *See* FTC, Press Release, FTC Investigation Leads to Lawsuit Against TikTok and ByteDance for Flagrantly Violating Children's Privacy Law (Aug. 2, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law; *see generally* 2023 Ransomware Report at 14-15 (describing the FTC's 2019 lawsuit and the resulting stipulated order).

complaint, TikTok Ltd.'s principal place of business is in Singapore or Beijing, China.[111] It also generally alleges the companies violated the 2019 order and continued to violate COPPA by knowingly allowing children under 13 to create and use TikTok accounts without their parents' knowledge or consent, thereby collecting personal information from children, and by failing to comply with parents' requests to delete their children's accounts and personal information.[112] For instance, TikTok allegedly had a policy of maintaining accounts of children that it knew were under 13 unless the child made an explicit admission of age and other rigid conditions were met.[113] The company allegedly continued to collect personal data from these underage users, including data that enabled TikTok to target advertising to them, without notifying their parents and obtaining their consent as required by the COPPA Rule.[114] The complaint further alleged that TikTok built back doors into its platform that allowed children to bypass the age gate aimed at screening children under 13.[115] Moreover, TikTok allegedly collected numerous categories of information and more data than needed, such as information about children's activities on the app and multiple types of persistent identifiers to build profiles on children, while failing to notify parents about the full extent of its data collection and use practices.[116] Furthermore, TikTok allegedly made it difficult for parents to request that their child's accounts be deleted, including by imposing unnecessary and duplicative hurdles and often failing to comply with parents' requests.[117] The complaint asked the court to impose civil penalties against the defendants and to enter a permanent injunction to prevent future violations of COPPA.[118]

In 2025, the FTC also alleged that Singapore-based Cognosphere Pte. Ltd.—an entity reportedly connected to Chinese video game development company, MiHoYo[119]—and its California-based

---

[111] *See United States v. Bytedance*, No. 24-cv-06535 (C.D. Cal. Aug. 2, 2024), ECF No. 1: Compl. ¶ 13, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/bytedance_complaint.pdf.). At the time, TikTok was owned and operated by the Chinese parent company ByteDance. It has since been the subject of a deal through which a new American entity would own and operate the company. *See TikTok finalizes a deal to form a new American entity*, APNews (Jan. 23, 2025), https://apnews.com/article/tiktok-deal-us-china-eccb46c3bfee4cf3d362a01fe4968a4f.

[112] *See id.* ¶ 3.

[113] *See, e.g.,* FTC, Press Release, FTC Investigation Leads to Lawsuit Against TikTok and ByteDance for Flagrantly Violating Children's Privacy Law (Aug. 2, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law; *United States v. Bytedance*, No. 24-cv-06535 (C.D. Cal. Aug. 2, 2024), ECF No. 1: Compl. ¶ 81, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/bytedance_complaint.pdf.

[114] *See, e.g.,* FTC, Press Release, FTC Investigation Leads to Lawsuit Against TikTok and ByteDance for Flagrantly Violating Children's Privacy Law (Aug. 2, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law.

[115] *See id.*

[116] *See id.*

[117] *See id.*

[118] *See id.*; *United States v. Bytedance*, No. 24-cv-06535 (C.D. Cal. Aug. 2, 2024), ECF No. 1: Compl. ¶¶ 4, 125, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/bytedance_complaint.pdf. The Commission referred the matter to the Department of Justice which filed the lawsuit in August 2024 and litigation is ongoing.

[119] *See, e.g.,* Kathryn Rattigan, Data Privacy and Cybersecurity Insider, Video Game Maker to Pay $20 Million to Settle FTC COPPA Enforcement Action (Jan. 23, 2025), https://www.dataprivacyandsecurityinsider.com/2025/01/video-game-maker-to-pay-20-million-to-settle-ftc-coppa-enforcement-action/ (referring to Cognosphere as a "Singapore-based Chinese video game developer"); Sophie McEvoy, GamesIndustry.biz, Cognosphere to pay $20m to settle FTC complaint on Genshin Impact (Jan. 20, 2025), https://www.gamesindustry.biz/cognosphere-to-pay-20m-to-settle-ftc-complaint-on-genshin-impact ("Cognosphere is a subsidiary of Chinese developer MiHoYo and publisher of Genshin Impact."); Kanishka Singh, Reuters, 'Genshin Impact' publisher settles US charges of violating children's privacy (Jan. 17, 2025), https://www.reuters.com/technology/genshin-impact-maker-settles-us-charges-violating-childrens-privacy-2025-01-17/ ("The [Genshin Impact] game was made by Chinese developer MiHoYo.").

subsidiary Cognosphere LLC (collectively, Cognosphere), the makers of popular video game Genshin Impact, violated the FTC Act and COPPA.[120] The complaint alleged that Cognosphere actively marketed Genshin Impact to children and collected and used their personal information without parental consent, in violation of COPPA.[121] According to the complaint, Cognosphere deceived players about the odds of winning specific more highly sought-after loot box prizes and how much it would cost to open loot boxes to win the prizes.[122] Furthermore, Cognosphere allegedly promoted these prizes to children and allowed underaged users to purchase virtual currency without parental consent, which in some instances led children and teenagers to spend hundreds or thousands of dollars in pursuit of prizes.[123] As part of a settlement, Cognosphere agreed, among other relief, to pay $20 million in fines and to block children under the age of 16 from making purchases without parental consent.[124]

Similarly in 2023, the FTC took action against education technology provider Edmodo for allegedly collecting personal data from children without obtaining parental consent and using that data for advertising, in violation of COPPA, and for unlawfully outsourcing its COPPA compliance responsibilities to schools.[125] Edmodo's parent company NetDragon is reportedly a Chinese company listed on the Hong Kong stock exchange.[126] A stipulated order requires Edmodo to pay $6 million in monetary penalties (suspended due to the company's inability to pay) and contains protections for children's data should Edmodo resume operations in the United States, including mandating that the company to meet several conditions before obtaining school authorization to collect information from a

---

[120] *See* FTC, Press Release, Genshin Impact Game Developer Will be Banned from Selling Lootboxes to Teens Under 16 without Parental Consent, Pay a $20 Million Fine to Settle FTC Charges (Jan. 17, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/genshin-impact-game-developer-will-be-banned-selling-lootboxes-teens-under-16-without-parental.

[121] *See United States v. Cognosphere, LLC*, No. 25-cv-00447 (C.D. Cal. Jan. 17, 2025), ECF No. 1: Compl., *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/cognosphere_complaint.pdf; *see e.g., id.* ¶¶ 3, 4.

[122] *See id.* ¶ 6.

[123] *See id.* ¶ 9.

[124] *See* FTC, Press Release, Genshin Impact Game Developer Will be Banned from Selling Lootboxes to Teens Under 16 without Parental Consent, Pay a $20 Million Fine to Settle FTC Charges (Jan. 17, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/genshin-impact-game-developer-will-be-banned-selling-lootboxes-teens-under-16-without-parental; *see also United States v. Cognosphere, LLC*, No. 25-cv-00447 (C.D. Cal. Jan. 17, 2025), ECF No. 3-3, Proposed Stip. Order, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Cognosphere-Attachment3-3.pdf.

[125] *See* FTC, Press Release, FTC Says Ed Tech Provider Edmodo Unlawfully Used Children's Personal Information for Advertising and Outsourced Compliance to School Districts (May 22, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ed-tech-provider-edmodo-unlawfully-used-childrens-personal-information-advertising.

[126] *See, e.g.,* NetDragon – About, https://www.netdragon.com (last accessed Dec. 10, 2025) ("NetDragon Websoft Holdings Limited (HKSE: 0777) is a leading innovator and a creative force in China's online gaming and mobile internet industries."); PR Newswire, Edmodo Announced Closure of its B2G Version to Focus on Country Rollout Opportunities (Aug. 18, 2022), https://www.prnewswire.com/news-releases/edmodo-announced-closure-of-its-b2c-version-to-focus-on-country-rollout-opportunities-301608283.html#:~:text=HONG%20KONG%2C%20Aug.,learning%20vision%20of%20the%20Company ("NetDragon is one of the most reputable and well-known online game developers in China."); Sean Cavanagh and Sarah Schwartz, EdWeek Market Brief, Chinese Gaming Giant NetDragon Acquired Edmodo for $137 Million (Apr. 10, 2018), https://marketbrief.edweek.org/education-market/chinese-gaming-giant-netdragon-acquires-edmodo-for-137-million/2018/04 ("NetDragon was launched in 1999 and is based in Fuzhou, China.").

child and prohibiting the company from using children's information for non-educational purposes such as advertising or building user profiles.[127]

B. Fraud and Other Deception Enforcement Actions

The FTC targets scams and fraud.[128] These efforts include providing consumers with education resources and the ability to submit reports of suspected fraud, which the FTC uses to inform investigations and also shares with more than 2,800 law enforcers, who also use the reports to inform their own enforcement activities.[129] The most commonly reported types of fraud in 2024 were imposter scams; online shopping and negative reviews; business and job opportunities; investments; and internet services.[130] Here too, the Commission has in the past encountered links to China in its enforcement work, as well as some indications of the potential involvement of actors from Russia.[131]

The FTC is responsible for enforcing multiple laws that address false, misleading, or unsubstantiated "Made in the USA" or country-of-origin claims, including Section 5 of the Federal Trade Commission Act,[132] the Made in USA Labeling Rule,[133] and other laws and rules addressing specific product categories (e.g., textile, wool, and fur products) that expressly require disclosures about the country where the product was processed or manufactured.[134] FTC staff also collaborates with sister agencies, such as the U.S. Customs and Border Protection, which enforces laws and regulations requiring foreign-made products imported in the United States to have proper country-of-origin marking.[135]

The FTC has a longstanding history of pursuing law enforcement against companies who allegedly make false or unsubstantiated Made in USA claims about their products. In some cases, FTC staff has

---

[127] *See* FTC, Press Release, FTC Says Ed Tech Provider Edmodo Unlawfully Used Children's Personal Information for Advertising and Outsourced Compliance to School Districts (May 22, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ed-tech-provider-edmodo-unlawfully-used-childrens-personal-information-advertising; *see also United States v. Edmodo*, No. 23-cv-02495 (N.D. Cal. June 27, 2023), ECF No. 15: Stip. Order, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Edmodo-Dkt15%28Order%20Signed%20by%20the%20Court%29.pdf.

[128] *See, e.g.,* FTC, Bureau of Consumer Protection, Fighting Scams and Fraud, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection (last accessed Dec. 10, 2025).

[129] *See* FTC, Report to Help Fight Fraud!, https://reportfraud.ftc.gov/#/ (last accessed Dec. 10, 2025); *see also* FTC, Why Report Fraud?, https://www.ftc.gov/media/why-report-fraud-0 (last accessed Dec. 10, 2025).

[130] *See* FTC, A Scammy Snapshot of 2024, *available* at https://www.ftc.gov/system/files/ftc_gov/images/csn-scammy-snapshot-2024.png (last accessed Dec. 10, 2025); Press Release, FTC, New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024 (March 10, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.

[131] *See* 2023 Ransomware Report at Section II.B. (providing historical examples of FTC fraud enforcement actions involving actual and possible connections to China and Russia).

[132] 15 U.S.C. § 45.

[133] 16 C.F.R. Part 323. The Rule, which has been in effect since August 2021, prohibits the labeling of any product as "Made in the United States" unless (1) the final assembly or processing of the product occurs in the United States, (2) all significant processing that goes into the product occurs in the United States, and (3) all or virtually all ingredients or components of the product are made and sourced in the United States. *Id.*

[134] *See* Rules and Regulations under the Wool Products Labeling Act of 1939, 16 CFR Part 300; Rules and Regulations under the Textile Fiber Products Identification Act, 16 CFR Part 303; and Rule and Regulations Under Fur Products Labeling Act, 16 CFR Part 301.

[135] *See*, *e.g.*, Marking of Imported Articles and Containers, 19 U.S.C. § 1304; Part 134 – Country of Origin Marking,19 C.F.R. Part 134; *see also* U.S. Customs and Border Protection, "Marking of Country of Origin on U.S. Imports" (May 22, 2024*), available at* https://www.cbp.gov/trade/rulings/informed-compliance-publications/marking-country-origin-us-imports.

determined that the product at issue has links to the PRC. In this reporting period, for example, the FTC pursued law enforcement action against *Old Southern Brass*, a novelty products retailer, alleging among other things that it falsely claimed, both on its own website and on Amazon.com, that certain products were manufactured in the U.S. when they were wholly imported from the PRC at the time.[136] As part of a settlement, the company agreed to pay $150,000 to the FTC, stop making false Made in the USA claims, comply with specific requirements relating to future country-of-origin claims, and notify consumers of the false claims.

In addition, companies already under FTC Order face steep penalties for similar violations. In April 2024, the FTC alleged that William Sonoma made false or deceptive "Made in USA" claims for products including mattress pads wholly imported from the PRC, in violation of an existing FTC Order regarding Made in USA claims.[137] In that case, the FTC obtained a record civil penalty of $3.175 million.[138]

Separately, the FTC aims to eliminate false or misleading information from the marketplace and sometimes sends letters, by itself or jointly with other enforcement agencies, to warn companies that their conduct may be unlawful and that they could face legal consequences if they do not stop it.[139] The Commission has previously sent warning letters to entities with links to the PRC.[140]

III. Cross-Border Cooperation

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."[141] As detailed in the 2023 Ransomware Report and below, the FTC has had limited interactions with government agencies in some of the four countries covered by this report and is aware of only little or no direct enforcement cooperation on ransomware or cyber-related attacks.[142]

---

[136] *See* FTC, Press Release, FTC Finalizes Order Requiring Old Southern Brass to Stop False Made In USA and Veteran Affiliation Claims (Jan. 23, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-finalizes-order-requiring-old-southern-brass-stop-false-made-usa-veteran-affiliation-claims; *In the Matter of EXOTOUSA LLC*, Fed Trade Comm'n 2323035, Compl. at ¶¶ 5, 14, 17, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/EXOTOUSAComplaint.pdf. The complaint also alleged that the company falsely claimed that it was veteran-owned and that it donated 10 percent of its sales to military service charities. *See e.g., id.* ¶ 10.

[137] FTC, Press Release, Williams-Sonoma Will Pay Record $3.17 Million Civil Penalty for Violating FTC Made in USA Order (Apr. 26, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/04/williams-sonoma-will-pay-record-317-million-civil-penalty-violating-ftc-made-usa-order.

[138] *See id.*

[139] *See* FTC, About FTC Warning Letters, https://www.ftc.gov/news-events/topics/truth-advertising/about-ftc-warning-letters (last accessed Dec. 10, 2025).

[140] *See* 2023 Ransomware Report at Section II.C. (describing the FTC's issuance of warning letters to entities with links to China for apparently collecting children's location information without parental consent and for advertising that certain products treated or prevented Coronavirus Disease 2019 (COVID-19) without competent and reliable scientific evidence).

[141] *See* Consolidated Appropriations Act, 2023, Division BB, Title V, Public Law No: 117-328, *available at* https://www.congress.gov/117/plaws/publ328/PLAW-117publ328.pdf.

[142] *See* 2023 Ransomware Report at Section III.

FTC staff has had no interaction with agencies in either Iran or North Korea.[143] American consumers, as shown in the complaints analysis below, do not frequently report interactions with businesses in these countries.[144] 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 […] has repeatedly provided support for acts of international terrorism […]."[145] The Secretary of State has made that determination for Iran and North Korea during the time period covered by this report.[146]

Similarly, in this reporting period, FTC staff had no direct interactions with agencies in Russia. Again, U.S. consumer complaints relating to Russia have been relatively few in number.[147]

FTC staff had limited direct contact with a PRC government consumer protection agency. In the margins of a gathering of the International Consumer Protection and Enforcement Network (ICPEN) in Washington, D.C., in 2024, FTC staff met informally with the PRC's State Administration for Market Regulation (SAMR) at their request to hear about the FTC's general procedures for handling and processing consumer complaints. At that meeting, SAMR proposed negotiating a memorandum of understanding with the FTC involving voluntary enforcement assistance, information sharing, and other cooperation on consumer protection matters. However, no further engagement on these or other consumer protection topics occurred.

FTC staff has participated in multilateral fora on consumer policy and privacy where staff is aware that Chinese, Russian, and Iranian agencies have at times also participated.[148]

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 annually,[149] consumer reports about ransomware and other cyber-related attacks comprise only a small fraction of

[143] *See id.*
[144] In this reporting period, there were 309 complaints filed by US consumers regarding businesses believed to be located in Iran or North Korea, which represents 0.007% of all complaints filed by US consumers.
[145] *See* 5 U.S.C. § 46(j)(7).
[146] *See* U.S. Dept. of State, State Sponsors of Terrorism, https://www.state.gov/state-sponsors-of-terrorism/ (last accessed Dec. 10, 2025).
[147] In this reporting period, there were 1,123 complaints filed by US consumer regarding businesses believed to be located in Russia, which represents 0.027% of all complaints filed by US consumers.
[148] 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 (2013-25); Asia Pacific Economic Cooperation forum (APEC); and Global Privacy Assembly (GPA) (formerly the International Conference of Data Protection and Privacy Commissioners).
[149] The FTC collects and 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 July 1, 2023, to June 30, 2025 (loaded August 1, 2025). The information provided by consumers is self-reported and is not verified by the FTC.

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 July 1, 2023, and June 30, 2025, the FTC received over five million consumer fraud reports, over half a million of which (10.6%) were cross-border.[150] These reports show that U.S. consumers encounter significant fraud from outside the United States, with more than 144,000 consumers reporting an incident of cross-border fraud during this period. U.S. consumers also report significant financial injury from cross-border fraud – over $1.5 billion during this period and over $5.9 billion since 2006.[151]

As detailed below and in the 2023 SAFE WEB Report, consumer reports show that the PRC is a leading source of cross-border complaints. Those complaints, however, rarely concern ransomware or other cyber-related attacks.[152] Between July 1, 2023, and June 30, 2025, the FTC received 42,972 reports about fraud originating in the PRC, but *less than 1%* of these reports (0.24%) were related to ransomware or other computer exploits. And while consumers report more incidents of tech support scams – a type of fraud akin to ransomware – such reports nevertheless comprise *less than 3%* (2.78%) of the fraud reports about the PRC during this period. Instead, when consumers report about fraud originating in the PRC, they are largely concerned with issues related to *online shopping*, which account for *over 66%* of all such complaints.[153]

Consumers have also reported misconduct they believe originated in Russia, Iran, and North Korea, but less often than China. Complaints about misconduct originating in North Korea and Iran are infrequent. *Combined*, consumers have filed 2,515 fraud reports about these three countries between July 1, 2023, and June 30, 2025 – *0.05% of all fraud reports* received by the FTC during this period. When consumers do report harmful conduct originating in these countries, some of these complaints involve tech support scams, but reports of tech support scams originating in Russia and North Korea have both fallen over the last two years. While reports about malware and other computer exploits are uncommon for all three countries, the number of reports about malware exploits originating in Russia has increased over the last two years.[154]

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 two years since July 1, 2023, only *2.23% of all fraud reports* have concerned such issues. And, when reporting about such attacks, the majority of U.S. consumers – almost 95% – report that the attack either originated within the United States or do not report a location.

---

[150] 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.
[151] *See* 20233 Ransomware Report at 22 (reporting a total financial injury of $4.4 billion from 2006 to June 2023); *see also* 2023 SAFE WEB Report.
[152] Here, China includes reports about Hong Kong and Macau, which are tracked separately in Consumer Sentinel.
[153] *See* 2023 SAFE WEB Report at Section I and Appendix A.
[154] As detailed in the 2023 RANSOMWARE Report, from January 1, 2019, to June 30, 2023, there were 119 complaints about malware exploits originating in Russia, which averaged to 26.44 per year. *See* 2023 Ransomware Report at 30. In this reporting period, there were 80 complaints of malware exploits originating in Russia, which averaged to 40 per year, a 51.3% increase from the previous reporting period.

Reports about tech support scams are more prevalent – 2.45% 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 94% – also either identify the United States as the country of origin or do not report the origin country. In this reporting period, U.S. consumers most frequently identified Canada as the source of cross-border tech support fraud. The FTC has devoted enforcement resources to tech support scams, including those originating overseas, *see supra* Section I.B.[155] In the previous reporting period, when U.S. consumers did identify a foreign source of tech support fraud, which unlike ransomware attacks often involves telemarketing, they most frequently identified India as the source of cross-border tech support fraud.[156]

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 entities[157] 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 factors. First, as a general matter, consumers often do not file complaints, especially with the government; when they do file complaints, they often do so with entities directly involved in a transaction like a seller or manufacturer, a credit card company, bank, or other payment service provider.[158] In addition, consumers typically do not know where the entities perpetrating these attacks are located. Foreign scammers often mislead consumers about or conceal their locations through various techniques.[159] 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.[160]

---

[155] *See also* 2023 Ransomware Report at Section I.B.

[156] *See* 2023 Ransomware Report at 23. The FTC has worked with authorities in India and elsewhere to crack down on such scams. *See id.*; *see also* FTC, Press Release, 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, *Pecon Software Ltd., et al.* (Jul. 2014), *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/1123118-pecon-software-ltd-et-al; FTC, *Lakshmi Infosoul Services Pvt Ltd.* (Jul. 2014), *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/1223245-lakshmi-infosoul-services-pvt-ltd.

[157] In this report, "entities" refers to both companies and individuals.

[158] *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).

[159] *See* 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).

[160] 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. Furthermore, as

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 in enforcement actions and uses aggregate complaint data to report publicly on trends.[161] However, the FTC does not act upon each individual complaint received, directly or indirectly, given the millions of consumer complaints received each year. The 2023 SAFE WEB report to Congress describes this system in greater detail.[162]

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] Another important source is econsumer.gov, a project started in 2001 by members of ICPEN.[164] Through the econsumer.gov website, consumers can file cross-border reports and learn other steps to take to combat fraud, now available in 9 languages. Econsumer.gov receives tens of thousands of complaints each year. The FTC also receives consumer reports from other federal, state, local, and foreign law enforcement agencies, and certain organizations.[165] The FTC retains this data in the Consumer Sentinel Network, a secure online database available only to registered law enforcement agencies and users.[166] The fraud complaints housed in Sentinel are currently categorized into 17 categories and 47 subcategories.[167]

B. Consumer Sentinel Complaints about Malware and Tech Support Scams

Consumer Sentinel tracks information about "Malware & Computer Exploits" and "Tech Support Scams," which are relevant for 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

---

noted above, the FBI positions itself as the lead federal agency for investigating cyber attacks and intrusions. S*ee* FBI, What We Investigate, https://www.fbi.gov/investigate/cyber (last accessed Dec. 11, 2025). The FBI also collects consumer complaints through its Internet Crime Complaint Center (IC3). *See* FBI, Internet Crime Complaint center, https://www.ic3.gov/Home/ComplaintChoice (last accessed Dec. 11, 2025). The FBI's IC3 also prepares annual reports summarizing its complaints. *See* FBI, Internet Crime Complaint Center, Annual Reports, https://www.ic3.gov/AnnualReport/Reports (last accessed Dec. 11, 2025). The following summarizes the number of ransomware complaints received with adjusted monetary losses: 2023 (2,825 complaints and losses of over $59.6 million); 2024 (3,156 complaints and losses of over $12.5 million). *Id*.

[161] Additional information on how the FTC uses consumer complaints is located in Appendix B of the 2023 SAFE WEB Report.

[162] *See* Appendix B of the 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] *See generally* www.econsumer.gov.

[165] 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 Dec. 11, 2025).

[166] *See* FTC, Consumer Sentinel Network, https://www.ftc.gov/enforcement/consumer-sentinel-network (last accessed Dec. 11, 2025).

[167] Sentinel category descriptions are available at FTC, Consumer Sentinel Network, https://www.ftc.gov/system/files/attachments/data-sets/category_definitions.pdf (last accessed Dec. 11, 2025). Sentinel subcategory definitions are available at FTC, Consumer Sentinel Network Subcategory Definitions (Oct. 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/CSNPSCFullDescriptions.pdf (last accessed Dec. 11, 2025).

about spyware, adware, and other types of malware, as well as denial of service attacks, some of which may be beyond the scope of Congress's inquiry.[168] 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.[169] Thus, while fraud is generally underreported, complaints under both of these categories cannot be relied upon to accurately measure ransomware fraud.[170]

1. Malware and Computer Exploits

The FTC has received relatively few consumer reports about malware and computer exploits, cross-border or otherwise. During the two years from July 1, 2023, and June 30, 2025, the FTC received 128,199 such reports, about a fifth of which were cross-border. Consumer complaints about such attacks and exploits accounted for *only 2.38%* of the fraud complaints the FTC collected during this period.

When consumers do report about such attacks, the vast majority – almost 95% – report that the attack either originated from the United States or do not report a location.[171] 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 1,928 complaints since July 1, 2023 (this represents 35.97% of all U.S. consumer cross-border complaints and 1.83% of all U.S. consumer complaints). Other reported countries in that same time period include Nigeria, which was identified by U.S. consumers in 719 complaints (13.41% of U.S. consumer cross-border complaints and 0.68% of all U.S. consumer

[168] The subcategory of "Malware & Computer Exploits" is defined as "Reports about computer software that gathers consumer information without consumer knowledge and/or consent. This includes spyware that receives information about consumers, such as browsing and Internet usage habits, and adware that displays advertising banners, redirects consumers to websites, and conducts other forms of advertising. Reports about malicious software that harms consumers' computers or software, including viruses, Trojans, and worms, as well as ransomware 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 take control of computers." *See* Consumer Sentinel Network Subcategories, Subcategory 52, https://www.ftc.gov/system/files/ftc_gov/pdf/CSNPSCFullDescriptions.pdf (last accessed Dec. 11, 2025). That subcategory along with the subcategory of "Privacy & Data Security" are part of a larger category of complaints about "Privacy, Data Security, and Cyber Threats." *See* Consumer Sentinel Network, Descriptions of Report Categories at 4, https://www.ftc.gov/system/files/attachments/data-sets/category_definitions.pdf (last accessed Dec. 11, 2025).

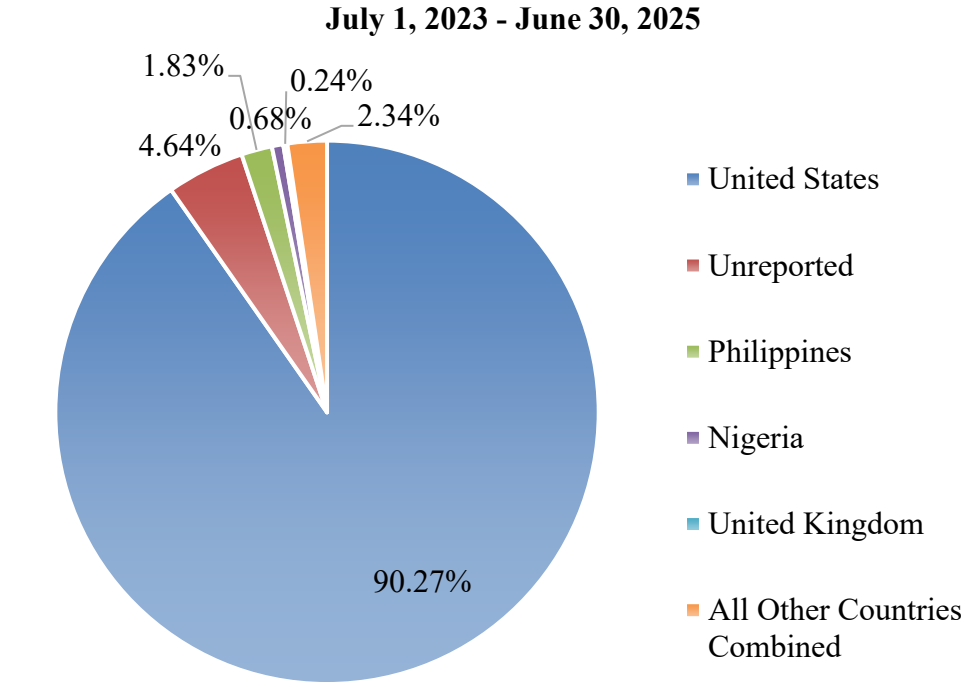
[169] The subcategory of "Tech Support Scams" is defined as "Reports about a scammer who claims to be a computer technician associated with a well-known company or its products. This individual will say viruses or other malware have been detected on consumers' computers and that remote access is needed 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 or smartphone." *See* Consumer Sentinel Network Subcategories, Subcategory 85, https://www.ftc.gov/system/files/ftc_gov/pdf/CSNPSCFullDescriptions.pdf (last accessed Dec. 11, 2025). "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. *See* Consumer Sentinel Network, Descriptions of Report Categories at 1, https://www.ftc.gov/system/files/attachments/data-sets/category_definitions.pdf (last accessed Dec. 11, 2025).

[170] When consumers report identify 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 near 6 million reports of identity theft that the FTC received between January 1, 2023, and June 30, 2025, less than 500 of them included the phrase "ransom." Of these, no consumers identified China, Russia, North Korea, or Iran as the country of origin.

[171] When reporting about such frauds, 93.9% of all consumers and 94.9% of U.S. consumers either report the United States as the source of the fraud or do not report a location.

complaints), and the United Kingdom, which U.S. consumers identified in 254 complaints (4.74% of U.S. consumer cross-border complaints and 0.24% of all U.S. consumer complaints). (*See Figure 1.*)

Figure 1: Top Country for Malware & Computer Exploits Complaints as Reported by U.S. Consumers
Source: FTC Consumer Sentinel Network Data

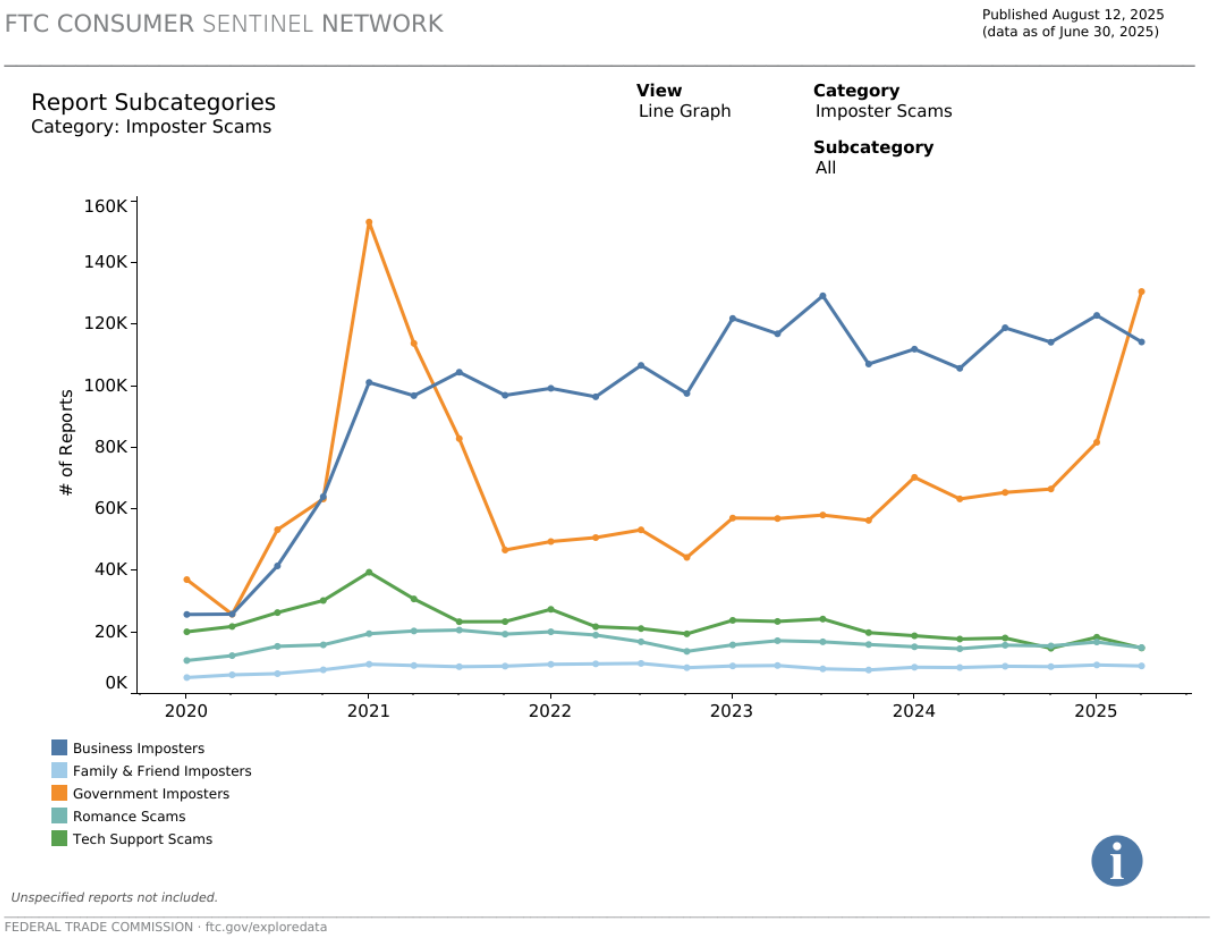


2. Tech Support Scams

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 July 1, 2023.[172] 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 reported less often than other types of imposter scams. (*See Figure 2.*) Since July 1, 2023, the FTC received 141,185 reports about tech support scams, *2.46% of all fraud reports* for this period. Of these reports, 10.88% of them were cross-border and 78.86% were filed by U.S. consumers.

[172] During this period, consumers reported 1,682,368 incidents of imposter scams, 34% of all fraud reports received by the FTC. Collectively, when consumers report about imposter scams, most (between 77% and 80% each year) do not report a financial loss. Those who do, however, report median losses ranging from $609 to $754.

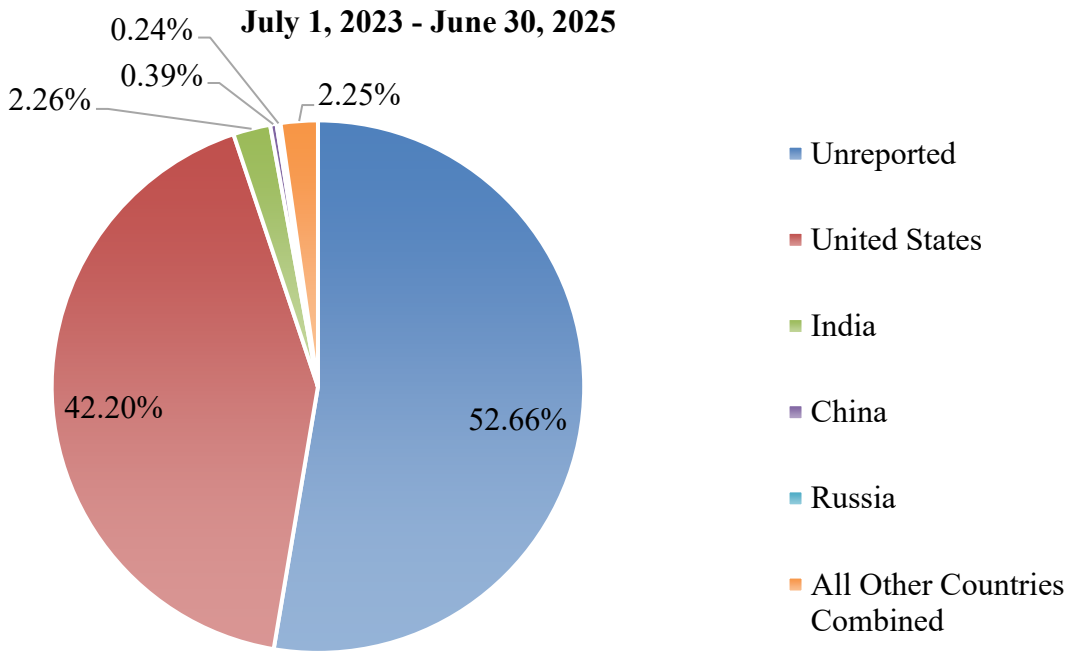
Figure 2: Reported Subcategories Over Time



Similar to consumer complaints about malware and 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, 82.32% of consumers report the location as the United States or do not report a location.[173] The overwhelming majority of American consumers – 94.85% – 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.

[173] Consumers may not know that a foreign entity is involved as, for example, foreign scammers often mislead consumers about or conceal their locations through various means, including using phone numbers that appear to be from the U.S., spoofing, fake social media profiles, and other tactics. *See* 2023 SAFE WEB Report at 6.

Figure 3: Top Countries for Tech Support Scam Complaints as Reported by U.S. Consumers
Source: FTC Consumer Sentinel Network Data



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 44% 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.[174] Other countries that have been associated with tech support scams include China and Russia, *see supra Figure 3* and *infra* Section IV.C. In total, U.S. consumers filed 5,730 cross-border reports about tech support scams since July 1, 2023.

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 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.[175]

---

[174] *See, e.g.,* 2023 Ransomware Report at 7-9; U.S. Attorney's Office, District of New Jersey, Press Release, 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.

[175] US consumers filed 31,253 complaints regarding fraud originating in China, compared to 1,423 complaints about fraud originating in Russia, Iran, or North Korea.

1. China

Between July 1, 2023, and June 30, 2025, consumers reported 42,972 incidents of fraudulent business conduct originating in China. This number constitutes 0.80% of the overall number of fraud complaints received during this period and 7.51% of the overall number of cross-border fraud complaints received. The vast majority of these reports (94.45%) were cross-border, with 31,253 (72.73%) of the total reports having been filed by U.S. consumers.[176] The nature of the fraud reported as originating in China is varied, covering nearly all fraud subcategories tracked by the FTC.[177]

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 3.02%* of reports about entities in China during this period, combined. Instead, when consumers report about fraud from China, most complaints, over 66%, are concerned with fraud related to online shopping, such as undisclosed costs, undelivered merchandise, and the failure to deliver ordered merchandise. (*See Figure 4*.) During this period, consumers filed 1,194 reports about tech support scams and 103 reports about malware and other computer exploits that they believed originated in China. Of these reports, U.S. consumers filed 90 complaints about malware and computer exploits and 429 complaints of tech support scams originating in China during this period.[178]

Figure 4: Consumer Sentinel Reports about Entities in China

Rank	Sentinel Fraud Category	Count	Percentage of Complaints
1	**Online Shopping**	**28,595**	**66.5%**
2	Business Imposters	5,932	13.8%
3	Miscellaneous Investments & Investment Advice	2,839	6.6%
4	Other Miscellaneous	1,975	4.6%
5	***Tech Support Scams***	***1,194***	***2.8%***
6	Government Imposters	654	1.5%
7	Job Scams & Employment Agencies	497	1.2%
8	Romance Scams	441	1.0%
9	Unsolicited Text Messages	430	1.0%
10	Unsolicited Emails	366	0.9%
	. . .		
15	***Malware & Computer Exploits***	***103***	***0.2%***

[176] Of the complaints filed about entities in China, 681 (1.55%) were filed by consumers who reported being in China, 1,703 (4.0%) did not report their location, and 31,253 (72.7%) were filed by consumers who reported being in the United States. The remaining 9,335 (21.75%) of complaints were cross-border complaints filed by other foreign consumers.
[177] *Cf.* 2023 SAFE WEB Report at Appendix A.
[178] 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, as some complaints may have been counted more than once.

2. Russia

Between July 1, 2023, and June 30, 2025, the FTC received 1,857 complaints about entities located in Russia. Of these reports, 1,581 (85.1%) were cross-border, with 1,123 (60.4%) of the total reports having been filed by U.S. consumers.[179] To put this number in context, U.S. consumers filed more than 27 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 more than a quarter of these complaints – a total of 518 (27.8%). (*See Figure 5*.) The FTC received 80 complaints (4.3%) from consumers about malware and other computer exploits originating in Russia. Of these reports, U.S. consumers filed 69 complaints about malware and computer exploits and 264 complaints of tech support scams originating in Russia since July 2023.[180]

Figure 5: Consumer Sentinel Reports about Entities in Russia

Rank	Sentinel Fraud Category	Count	Percentage of Complaints
1	***Tech Support Scams***	***518***	***27.9%***
2	Business Imposters	286	15.4%
3	Unsolicited Emails	231	12.4%
4	Miscellaneous Investments & Investment Advice	231	12.4%
5	Online Shopping	147	7.9%
6	Romance Scams	136	7.3%
7	Unsolicited Text Messages	132	7.1%
8	Government Imposters	98	5.2%
9	***Malware & Computer Exploits***	***80***	***4.3%***
10	Job Scams & Employment Agencies	79	4.2%

[179] Of the complaints filed about entities in Russia, 104 (5.6%) were filed by consumers who reported being in Russia, 172 (9.3%) did not report their location, and 1,123 (60.5%) were filed by consumers who reported being in the United States. The remaining 458 (24.7%) were cross-border complaints filed by other foreign consumers.
[180] 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, as some may have been counted more than once.

3. North Korea

Between July 1, 2023, and June 30, 2025, consumers reported 323 incidents of fraud originating in North Korea. Of these reports, 304 (94.1%) were cross-border, with 198 (61.3%) of the total reports having been filed by U.S. consumers.[181]

During this period, no reporting subcategory received over 100 complaints. Consumers filed 31 reports about tech support scams and 12 reports about malware or other computer exploits. (*See Figure 6.*) Of these reports, U.S. consumers filed 9 complaints about tech support scams and 10 about malware and other computer exploits that they reported as having originated in North Korea.[182]

Figure 6: Consumer Sentinel Reports about Entities in North Korea

Rank	Sentinel Fraud Category	Count	Percentage of Complaints
1	**Online Shopping**	**72**	**22.3%**
2	Romance Scams	68	21.1%
3	Miscellaneous Investments & Investment Advice	53	16.4%
4	***Tech Support Scams***	***31***	***9.6%***
5	Business Imposters	29	9.0%
6	Unsolicited Emails	16	5.0%
7	Job Scams & Employment Agencies	12	3.7%
8	***Malware & Computer Exploits***	***12***	***3.7%***
9	Government Imposters	11	3.4%
10	Unwanted Telemarketing Calls	10	3.1%

4. Iran

The FTC received 335 complaints about businesses located in Iran between July 1, 2023, and June 30, 2025. Of these reports, 141 (42.09%) were cross-border, with 111 (33.13%) of the total reports having been filed by U.S. consumers.[183]

[181] Of the complaints filed about entities located in North Korea, 198 (61.3%) were filed by consumers who reported being in the United States, 18 (5.6%) were filed by consumers who did not report their location, and a smaller number reported being in North Korea. The remaining complaints were cross-border complaints filed by other foreign consumers.
[182] 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.
[183] Of the complaints filed about entities located in Iran, 155 (46.3%) were filed by consumers who reported being from Iran, 39 (11.6%) did not report their location, and 111 (33.1%) reported being located in the United States. The remaining 30 (9.0%) were reported by other foreign consumers.

During this period, the only complaint category to exceed 100 complaints was miscellaneous investments and investment advice, with 111 complaints (33.1%). Consumers filed 27 reports about tech support scams and 7 reports about malware and other computer exploits that they believed originated in Iran. Of these reports, U.S. consumers filed 18 complaints about tech support scams and a smaller number were complaints about malware and other computer exploits that they reported as having originated in Iran. (*See Figure 7*.)

Figure 7: Consumer Sentinel Reports about Entities in Iran

Rank	Sentinel Fraud Category	Count	Percentage of Complaints
1	**Miscellaneous Investments & Investment Advice**	**111**	**33.1%**
2	Business Imposters	41	12.2%
3	Unwanted Telemarketing Calls	39	11.6%
4	Romance Scams	28	8.4%
5	Job Scams & Employment Agencies	27	8.1%
6	***Tech Support Scams***	***27***	***8.1%***
7	Government Imposters	22	6.6%
8	Online Shopping	13	3.9%
9	Unsolicited Emails	12	3.6%
10	***Malware & Computer Exploits***	***7***	***2.1%***

V. Legislative and Business Recommendations

The FTC submits the following recommendations for legislation that may assist the FTC in carrying out the U.S. SAFE WEB Act of 2006 or that could advance the security of the United States or American companies, and recommendations for American businesses and citizens to implement best practices to mitigate against such attacks, pursuant to Congress's direction in the RANSOMWARE Act.

First, the FTC again urges Congress to make the U.S. SAFE WEB Act permanent. As detailed in the 2023 SAFE WEB Report,[184] 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 would be significantly curtailed.

[184] *See* 2023 SAFE Web Report at Section III.

In addition, for many years the Commission relied on Section 13(b) of the FTC Act[185] for authority to obtain equitable monetary redress for consumers. Indeed, redress obtained under Section 13(b) accounted for the overwhelming majority of redress obtained for consumers in fraud cases. The Supreme Court, however, unanimously concluded in *AMG Capital Management v. FTC*[186] that Section 13(b) does not authorize courts to award monetary relief in Commission enforcement actions. Although the Commission believes that *AMG Capital Management* was correctly decided, that decision has removed a significant tool through which the FTC has historically obtained monetary redress for consumers. The Court's decision in that case, however, need not be the last word; Congress has the power to respond and enact legislation that does authorize the FTC to obtain equitable monetary redress for consumers—effectively restoring what the FTC had been using before *AMG Capital Management*. The FTC therefore continues to urge Congress to take action that would provide the FTC with the ability to seek monetary relief under Section 13(b) of the FTC Act so that the Commission can provide refunds to harmed consumers and prevent violators from benefitting from their schemes by keeping their illegally gained profits. The FTC looks forward to continuing to work with Congress to draft related appropriate language to protect consumers.

The Commission also continues to encourage Congress to enact privacy and data security legislation that is enforceable by the FTC, especially to protect children online.[187] Such privacy and data security legislation could also protect American consumers and businesses against ransomware and other cyber-related attacks.

Finally, businesses often serve as the front-line defenses against cyber attacks and are responsible for engaging in reasonable practices to safeguard consumer data. As a result, one of the most important ways to fight ransomware attacks is for businesses to take reasonable and appropriate steps to protect themselves and the data in their possession.[188] With regard to ransomware specifically, businesses should implement appropriate employee training, such as training employees to recognize and avoid phishing emails with links or attachments, which make up the majority of ransomware attacks. They should evaluate 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, businesses should take reasonable steps to have an appropriate plan in place to quickly respond to potential ransomware attacks in order to quickly mitigate the damage they can cause.

---

[185] 15 U.S.C. § 53(b).
[186] *AMG Capital Mgmt., LLC v. FTC*, 593 U.S. 67 (2021).
[187] *E.g.*, Keynote Speech of Chairman Andrew N. Ferguson at 9, The Attention Economy: How Big Tech Firms Exploit Children and Hurt Families (June 4, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/andrew-n-ferguson-keynote-attention-economy-06-04-25.pdf.
[188] *See, e.g.,* FTC, Data Security, https://www.ftc.gov/business-guidance/privacy-security/data-security (last accessed Dec. 10, 2025).

Acknowledgments

This report was drafted by Angel Martinez, Abigail Miller, and Laureen Kapin of the FTC's Office of International Affairs. Additional acknowledgement goes to Anne Miles and the FTC's Division of Consumer Response and Operations as well as the staff of the FTC's Bureau of Consumer Protection.