Executive Summary

The FTC respectfully submits this report as directed by the "Reporting Attacks from Nations Selected

Section I summarizes FTC activities addressing ransomware and other cyber-related attacks. This includes enforcement against data security practices that leave consumers or their data vulnerable to ransomware and other cyber-related attacks. It also covers enforcement actions concerning tech support scams, which sometimes involve taking control of consumers' computers and then demanding a ransom payment. Complementing this enforcement work is FTC consumer and business education about how to spot and avoid such harms and the FTC's outreach to and cooperation with foreign partners.[4]

Section II describes additional FTC enforcement actions involving China and Russia, including on privacy, data security, fraud and other deception, as well as warning letters to Chinese companies.

Section III addresses cross-border cooperation on the subjects described in the report with government agencies in China and Russia.[5]

Section IV provides consumer complaint data and trends related to ransomware and other cyber-related attacks, tech support scams, and individuals, companies or governments with ties to the four countries identified in the RANSOMWARE Act. The FTC provides further international complaint data in a companion report submitted at the same time to Congress: "The U.S. SAFE WEB Act and the FTC's Fight Against Cross-Border Fraud."[6]

Section V offers legislative recommendations to advance the FTC's mission in carrying out the U.S. SAFE WEB Act,[7] and to protect the security of the United States and U.S. companies against ransomware and other cyber-related attacks. The section also offers best practice recommendations for U.S. businesses and consumers dealing with such threats.

[4] The FTC has not engaged in foreign litigation regarding the topics identified in the RANSOMWARE Act.
[5] The FTC has not engaged in cooperation with North Korea or Iran.
[6] *See* FTC, The U.S. SAFE WEB Act and the FTC's Fight Against Cross-Border Fraud (Oct. 20, 2023) ("FTC 2023 SAFE WEB Report") at Section I and Appendix A. FTC reports are available at https://www.ftc.gov/policy/reports/commission-staff-reports.
[7] Pub. L. No. 109-455, 120 Stat. 3372 (2006) (codified in scattered sections of 15 U.S.C. and 12 U.S.C. § 3412(e)). Congress also requested recommendations for legislation that may assist the FTC in carrying out the SAFE WEB Act in its 2020 law extending the Act until 2027. Pub. L. No. 116-173, 134 Stat. 837 (2020), *available at* https://www.congress.gov/116/plaws/publ173/PLAW-116publ173.pdf.

data. To date, the FTC has brought more than 80 enforcement actions involving data security. These actions have

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

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

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

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

[32] Companies occasionally inform us of their data breaches voluntarily and sometimes they are legally required to do so, such as under the Health Breach Notification Rule. *See* 16 CFR Part 318, *available at* https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule. The FTC is currently considering amendments to the Safeguards Rule to require financial institutions to report certain data breaches and other security events to the Commission. *See* 16 CFR part 314, *available at* https://www.federalregister.gov/documents/2021/ 1 .0041 (he16 (/)6.9 (1 .(20ch)]TJ0 Tc 0 Tw4..253 0 Td(-)Tj0.006 Tc -

suggesting that malicious actors involved in data breaches were located in China or Russia. For example, in *Equifax Inc.*, the FT (e)-6o-1 (w<(T)1 on4 Tm[(m)-2 (pl)-2a)4 (Tf[(he)4 C)-3 (hi)-2 n(i)-2 (c)4 mao (a

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

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

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

[53] *See id*. The FTC also worked with Microsoft (a Sentinel data contributor) and other computer companies.
[54] *See* Press Release, FTC, Federal Court Orders Tech Support Scammers to Pay More Than $5.1 Million (July 24, 2014), https://wcFe

roundtable in New Delhi to develop a long-term strategy for combatting various types of telemarketing fraud originating in India, including tech support scams. The roundtable brought together Indian and foreign law enforcement officials, as well as representatives from India's legitimate call center industry, technology companies, and consumer groups. The Canadian Radio-television and Telecommunications Commission and the United Kingdom's National Crime Agency also participated. The meeting ultimately led to the formation of a council of industry leaders and government officials dedicated to combatting Indian telemarketing fraud and the development of an action plan to address the problem. A follow-low-the the

A A

A A

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

The FTC, through public outreach, has informed and brought together key players on ransomware. In 2016, as part of a larger seminar series on emerging consumer technology issues, the FTC hosted a workshop focused on ransomware.[63] Recognizing that ransomwar(ogy i g/TT0w 19.12 0 T (or)3)-2 (s)-1 (, t)a Tw 20
to avoi.613 d them. The FTC 2 (s)-has also hosted webinars and other business focused events 20.3 0 Tw 5.613
departments to he5.613 p them navigate the-wor5.613 d of cybersecurin (e)y. T
networks and data in plain, c5.613 ear language that is easy to understand so tha
win (e)h their employees, vendors, and others about cybersecurin (e)y.

[65] These mat rials include a central and easily accessible-wsit that covers a range of cybersecurity topics such as ransomware (*see Photo 1*),[66] tech-support.613 scams,[67] and other cyber-related attaks, in both English and Spanish. [68] The FTC's business gui.613 danceTeffort.613 s e.o inc5.613 udeTblog posts, podcasts, vi.613 deos, and more. For examp5.613 published blogs on ransomware prevention,[69] vi.613 deos on defending against and responding to

---

[63] *See* FTC, Fall Technology Series: Ransomware, September 7, 2016, https://www.ftc.gov/news-events/events/2016/09/fall-technology-series-ransomware (last accessed Sept. 28, 2023).
[64] *See generally* Press Release, FTC, New Green Lights & Red Flags business seminar debuts in Atlanta (July 2, 2019), https://www.ftc.gov/business-guidance/blog/2019/07/new-green-lights-red-flags-business-seminar-debuts-atlanta (last 10.6 4.Tw (2 0.604 .Tw (22 5)3) 0.

from malware.[78] Similarly, the FTC has issued consumer alerts and published articles and infographics addressing various tech support scam issues. These have included advice on how to spot, avoid, and

security as well as fraud and other deception

In *Zoom* -

email addresses, and other personal information from users under the age of 13.[96] And user accounts were public by default, which meant that a child's profile bio, username, picture, and videos could be seen by other users, and there were public reports of adults tr

chargebacks from their credit card companies, they found that the defendants used falsified shipment information to make it harder for consumers to get the charges reversed.[115] The FTC obtained from a U.S. district court a temporary restraining order and a preliminary injunction, which effectively shut down approximately 100 fraudulent websites.[116] The Commission asked the court for time to find and serve the defendants,[117] but suad-4 ()4 (our)3 (t)-2 (y)-4 ( )]TJ0 Tc 0 TwiDC 0.0D 32 D 36 ɔ36 ƀBDC 0h (er)-1 (s)-5c

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

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

C. FTC Warning Letters to Chinese Companies

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

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

---

[127] *See id.*
[128] *See id.*
[129] *See id.*
[130] Press Release, FTC, FTC Takes Action Against Lions Not Sheep and Owner for Slapping Bogus Made in USA Labels on Clothing Imported from China (May 11, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-takes-action-against-lions-not-sheep-owner-slapping-bogus-made-usa-labels-clothing-imported.
[131] *See id.*
[132] *See id.*
[133] These matters include *Instant Brands, J55S-S SJ9l[(S)-4 (s)-2.6 (/4 (es)1Tj0.004 9 (nt)6 U37 0 Tdi0.004 Tc4.89(S)-4 d S)7nd MTc4.89(S*

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

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

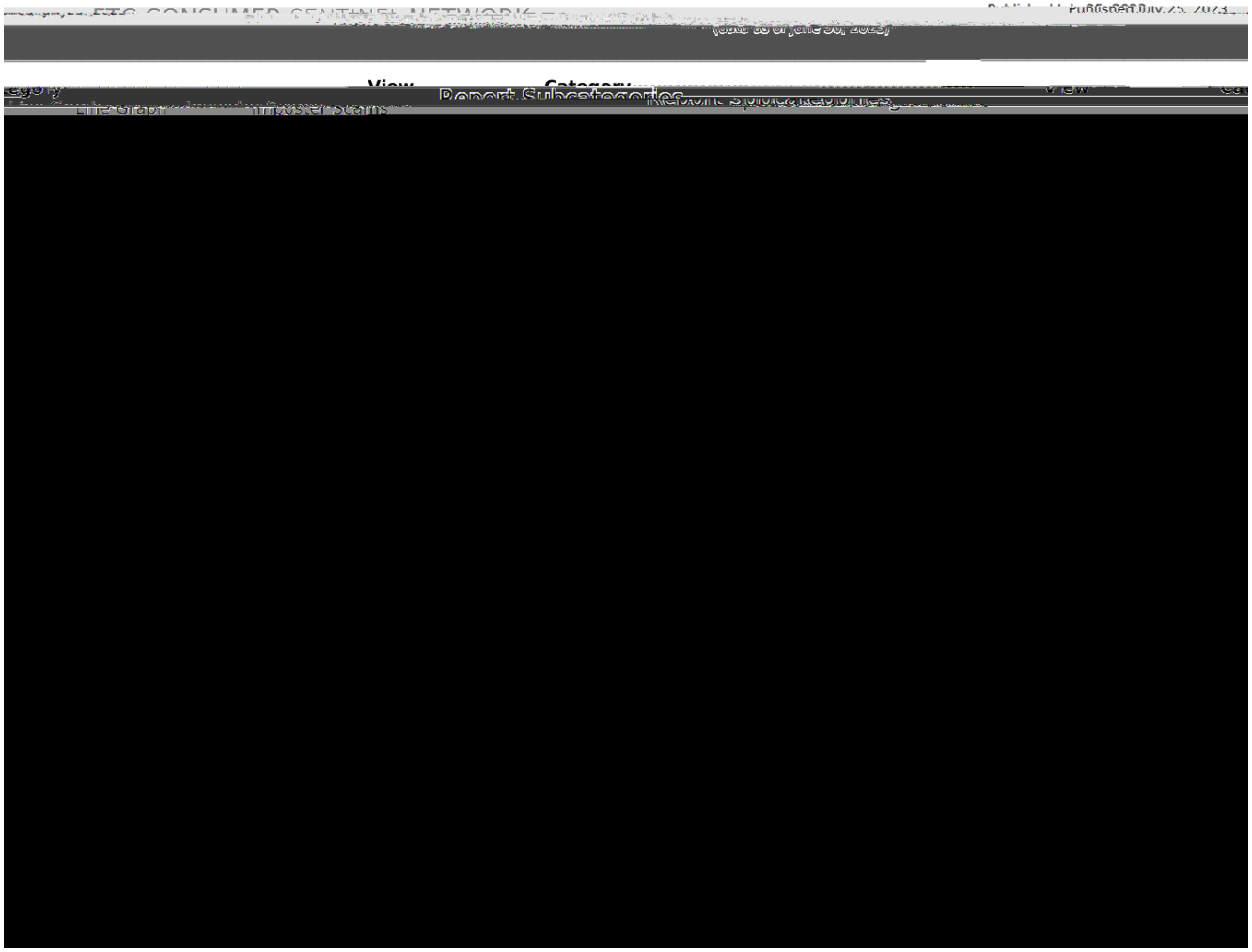
More recently, the FTC published an advisory (in English and Chinese) regarding a new investment scam targeting WeChat groups. According to the FTC the scam "stole millions from the Chinese community in the U.S.":

> Using WeChat groups, scammers heavily promoted the investment with pictures and stories about supposed successful investors. To invest, people agreed to over-pay upfront — as much as three times the retail price — to buy items like iPhones, laptops, and furniture. In exchange, scammers promised to return investors' money in 1-

IV. Consumer Complaint Data and Trends Related to Ransomware, Tech Suppo

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

Figure 2: Reported Subcategories Over Time



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

2. Russia

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

Consumer complaints about Russia are varied, covering most identified S (f)3 (i)-2 (e)4 (n)4 (d S)-416ied, auD 2 /M

The FTC's

In addition, the FTC urges Congress to amend Section 13(b) of the FTC Act[182] to restore the FTC's ability to

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

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