FILED

May 19 2020

SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND

ALDEN F. ABBOTT
General Counsel

RONNIE SOLOMON, Cal. Bar No. 284923
SARAH SCHROEDER, Cal. Bar No. 221528
Federal Trade Commission
901 Market Street, Suite 570
San Francisco, CA 94103
rsolomon@ftc.gov, sschroeder@ftc.gov
Tel: (415) 848-5100; Fax: (415) 848-5184

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

FEDERAL TRADE COMMISSION,

Plaintiff,

vs.

NTS IT CARE, INC., a California corporation, and

JAGMEET SINGH VIRK, individually, and as an owner, officer, and director of NTS IT Care, Inc.,

Defendants.

Case No. 4:20-cv-3388-PJH

FILED UNDER SEAL

DECLARATONS IN SUPPORT OF FTC'S MOTION FOR TEMPORARY RESTRAINING ORDER

VOLUME 6 OF 7

296	90375353	11/20/2017	Honolulu, HI	Consumer is calling to report she received a pop-up from someone claiming to be Microsoft and said her computer needed to be fixed. She did call the number and gave access to her computer. They gave her a virus on her computer. She found out the company was NTF IT Care Inc. She paid $432.96. Gave number to the CRA's.
297	87448648	11/21/2017	Piqua, OH	My mother [redacted], of Ohio, is an elderly person on a fixed (Social Security) income, who was duped by an illegal computer pop-up that included the trademarked Microsoft name in a misleading manner. She called the number provided in the pop-up, expecting to be speaking with someone at Microsoft. The person that she spoke with convinced her to pay $400 (via credit card) to resolve her computer issue. $400 might not be a lot of money to some, but it's very significant to someone who only has a small social security check to survive. I contacted the company, who are apparently based out of India. The representative refused to reverse the charges, claiming they are a legitimate business, and that they don't send pop-up messages. They offered to extort less money ($108) if I was willing to settle for that, I declined. I'm respectfully requesting that you look into the practices of this company, NTS IT Care, shut down their illegal activities, and get a 100% return of my mother's money. It's a sad day if your office ever considers this to be a legitimate business model; sending spyware to someone's computer so you can extort money from them, especially the elderly, despicable!
298	98318988	11/21/2017	Washington, CA	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number A42B1729-2FB7-4DE3-87AB-B748C2BEC230. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- My mother [redacted] of Ohio is an elderly person on a fixed (Social Security) income who was duped by an illegal computer pop-up that included the trademarked Microsoft name in a misleading manner. She called the number provided in the pop-up expecting to be speaking with someone at Microsoft. The person that she spoke with convinced her to pay $400 (via credit card) to resolve her issue. --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: false --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: 26-49
299	98328953	11/22/2017	Brea, CA	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 1E681EB3-A40F-44C9-BD67-E278A287F71F. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- This is my second report on this scam today. Per Intelius.com a person with the same name as the owner of NTS IT CARE INC is also current or former employee of Microsoft Corporation. That name is Jagmeet Virk Singh. The pop-up/hostage-ware includes Microsofts name in various places. My mother is elderly and fell victim to these thieves. Please follow-up on this matter. --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: 26-49
300	90638856	11/30/2017	-	DNC EMAIL - Forwarded from the FTC to the DNC email box. Consumer did not give complete contact info. Consumer sent screen shots of a company he did research on on the internet. This company is called NTS IT Care Inc, and they locked up his mothers computer and charged her $400 to unlock it. Consumer says he called them and demanded they refund her money, and they told him that for $108 they could stop it. Consumer research gives the owner of the company and indicates he used to work for Microsoft, which is who they claimed to be when they locked up the consumers mothers computer.
301	90638780	11/30/2017	Lisbon, NH	Consumer states that he responded to a pop up on his computer for major issues that were detected, called the phone # provided spoke to someone representing NTS IT Cares. Consumer granted the caller remote access to his computer and paid with his CC $227.89 for a two year tech support program. Consumer found address online.
302	98339488	12/2/2017	Brookville, PA	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number D68AE8DB-42A0-49CB-AFFB-F0134360FCA6. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- He did show me their website address but quickly and I didnt get to write it down. Also gave me this number to contact the Tech: 1-866-8115-9991 --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue --- Consumer Age Range: 50-65

303	98344098	12/4/2017	Whittier, CA	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted] It will help if you provide the Microsoft reference number 8CE0354F-45E6-4ECF-8960-C362A41CD6C5. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- I spoke to a person Brenda who provided her direct number as 1-844-208-2608 ext. 568. After checking my PC she said it had a virus and needed technical support to clean entire PC system and that I needed a firewall. She wanted to assigned a tech at cost of $199.00/year. She showed to me Microsoft website to prove they were a legit company. I refused her services. --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue --- Consumer Age Range: Over65
304	98312218	12/7/2017	Lebanon, OH	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 70F9E180-957F-4943-9328-5E57A50B1162. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- Pop Up Message / Computer Locked / Called Number Given (to Microwave?) / Was told I had a Zeus Virus and that I had not renewed my Firewall/ On the phone with them for over one hour and was told I needed to re-new my firewall ($400.00 for three years) and $49.99 for the maintenance service ? I charged it to my Visa card. My computer was then put back in service --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: Over65
305	90861327	12/8/2017	Blythewood, SC	The consumer got a message on their computer from someone posing as Microsoft stating that there were many viruses on the consumer's pc and needed access to the pc to remove the issues. The consumer allow the caller to access the pc. The caller then told the consumer that there would be a fee of $349 to upgrade the pc and fix the issue. The consumer did not pay the money.
306	91032487	12/13/2017	Burnsville, MN	a screen appeared on my computer as a security alert. I was instructed to call the phone number for instructions. the representative said he was a certified Microsoft agent and I had to let them clean my computer and install McAfee antivirus. It was scary. I did what the said and paid 289.24 for the service which they billed as McAfee. I checked a few days later and they were not connected to Microsoft in any way. I had Microsoft remove all the software they installed and cleared my entire harddrive. Their email is support@ntsitcare.com. I have had to change my bank accounts and all computer related information. I am having the bank initiate a dispute for the money charged to my credit card account. LindaTOPIC:Referrals
307	90984749	12/13/2017	North Tonawanda, NY	While browsing my email, a pop-up came up saying my computer was infected with viruses and froze. Computer would not function unless i called 1-844-208-2608 immediately and do not shut down computer or close internet until calling. An IT tech named Robert Cloud convinced me that I should allow him remote access to computer to clean viruses and promptly began to upsell me antivirus software etc. using intimidating tactics to give him my name, address, phone #, and of course my credit card number or my computer would be irrepairably damaged. I, being a disabled senior citizen fell for the ploy. He remotely created e-mails for me to send to him for authorizing said repair. I am not computer literate and again let him work his magic. I already had antivrus on my computer so i didn't know what to do. After they achieved my personal info including credit card number. They remotely accessed my printer and created a business like invoice and upcharged my credit card $499.99. After I told my family what had occurred, they said I was scammed and promptly PROVED it by checking with the BBB,FTC and videos posted by others with the same story. Including one recorded live verbatim. I was shocked. Cancelled credit card and called back demanding a refund. unsuccessfully of course. Anything you can do to help me recoup my loss would be helpful. Thank You.
308	91054277	12/14/2017	Rayville, MO	MAIL: The consumer's letter was forwarded by Attorney General of Missouri. Consumer reported receiving a phone call from NTS offering a refund from service she bought for her PC. Consumer was told to go to her PC for the refund. Consumer complied and could see the refund of $4000 in her account instead of the $400. Consumer was instructed to send back the $3600 ASAP. Consumer went to her back and done a bank transfer to this individual. After the consumer got home and checked her account she saw that the $4000 was gone. Consumer was told by her bank to call the police and the FTC.
309	91051974	12/14/2017	Tyler, TX	Contact made on my computer. Stated that I had a virus and entered my computer to correct virus. Charged my credit card $1399. I am now trying to cancelnthese charges.

310	91149505	12/18/2017	-	A red web page pulled up and an American sounding announcer came across my computer saying something to the degree that my computer may have been exposed to malware and I should call this phone number to fix it. It would not let me leave the webpage, would minimize the screen and only show the red web page. I called the number, spoke with an Indian sounding male who said he was with NTS. He made me feel guilty for not updating my firewall and warrenty protection plan on my computer then offered to sell me one and install it on my computer. I questioned him on being with Windows and he didn't give me a clear answer and again made me feel like I did something wrong that caused the malware to be on my computer. I paid them $200, gave access to my computer, and he said he'd work for 30-40 minutes then call me when it's finished. He transfered me to another employee, also with an Indian accent, and he verified my credit card information and showed me on my computer as he inputed my information. It was a very nondescript web page that said NTS. All the red flags made me concerned, I called a friend who saw online that it was scam, so I shut down my computer, canceled my credit card, and changed all my passwords. I did speak to one other male with an Indian accent named Eric. They continued to try to call me and I didn't answer. I did receive an email verifying my purchase but I have permanently deleted it already.TOPIC:Referrals
311	98312163	1/3/2018	Slidell, LA	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigato [redacted] at [redacted]. It will help if you provide the Microsoft reference number 79824C7D-52E1-4CF9-B318-B85614939DF6. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- I thought it was legit. I thought my computer I received on Christmas came with a protection plan. When the pop up came it repeatedly popped up tabs with a mail computer voice saying the warning message. I called tech number given and felt eery the whole time but the man named nick reassured to me he was not a scam. It was when he mentioned pricing plans that I discontinued the phone call --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: false --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue --- Consumer Age Range: 18-25
312	98476859	1/3/2018	Piqua, OH	See Attached Click here to Get the File - use the Password: FEEF60C9 https://bluecomplaints.bbb.org/attachment/?c=12566472 --- Additional Comments: DesiredSettlementID: Other (requires explanation)See Attached
313	98337356	1/6/2018	Clementon, NJ	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 4A36F7D8-406C-4FBA-A168-13B61EFC85D9. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- Bought a new computor on 12/31/2017 on Thursday got a message from microsoft of a serious problem my computor was frozen and I couldnt do anything with it not even shut it down they came on saying they were microsoft techs and would help me resolve the problem and it would cost me 128.17 with the tax. I said ok and my computor was alright after that I have more to say but no more room to. --- Method of Contact: Other --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: Over65
314	98334181	1/8/2018	Bowie, MD	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 6B3C71AE-C607-4DA0-A6B3-D6EBE437B980. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- I have payment confirmation statement they sent me to pay for the service. I even have the error code. They tried to offer me a plan for one year at $129 I declined. I spoke to more than one representative and stayed on the call and watched what was done remotely. I had to at times to tell them to leave my apps that were on the computer alone and just fix the problem of the trojan torpig virus --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue

315	110762873	1/12/2018	North Chelmsford, MA	Note: C is for consumer and R is for merchant. — I first became aware of this company on 11/8/17 at 14:30 when my computer screen froze and a voice alert said that my financial, facebook logs, and emails were being downloaded by this infection and to call the number on the screen to get help with this problem. I called the 877-490-6709 number and was greeted by 'eric' who told me that his firm was contracted by Microsoft to deal with this problem. He asked for access to my computer, which I gave, and proceeded to get rid of the 'problem' for me. I was told that I could subscribe to their service for a 400$ fee, which covered remote IT help for 3 years. Since I needed to work from my computer I paid the fee, but did not realize that I was not signing up for a legitimate service. I contacted my anti-virus company - PC Matic who informed me that this was actually an advertisement with a rotating script built into it to keep it alive and look like an infection. PC Matic advised me to run a TSA adware removal tool if this should happen again. I phoned the NTS help desk with the information from PC Matic and they denied that they had put the adware on my computer. I was attacked again on 1/6/18 at 16:30 pm by adware which I removed. — Complaint Status: Closed
316	98476860	1/18/2018	Bryan, TX	company deceptively convinced me to purchase a service contract for my computer using high-pressure tactics.On August 25, 2017, late morning, my computer started making very loud,irritating noises that I didn't know how to stop. A message appeared on the screen directing me to call a number for help. I called the number and spoke with Ryan Thompson who told me I needed a firewall for my computer and that my other safety programs were not necessary. He claimed that Microsoft had subcontracted with NTS IT to resolve this issue and there were subcontractors all over the country who were taking care of this problem. We were able to talk on-line and he was able to see what was on my screen. After a considerable time, he indicated that my computer was now fine and I should cancel my other services. I agreed to a 3 year contract at $329.99. I immediately received a receipt with my computerized signature on it. (time dated:2017-08-25 12:21:22-07000 Subsequently, I have learned that the company NTS, while appearing to be legitimate, has had several complaints similar to mine. Today, (1/16/2018) I went on the NTS website and filled out a 'contact me' form stating I expected a refund from them because of the deceitful, pressured sales pitch I received.The papers I originally received indicated a phone number of 844.208.2608.Document reference #ID4GI9I6SL4677EIAZZK4IPARTY ID:BLMPTGIT8LTTPWL5UT4J75IP ADDRESS: 50.24.176.52 — Additional Comments: -Refund of $329.99-Cancellation of services-Removal of all identifying information on me from their records
317	92014175	1/19/2018	Brooklyn, NY	I am writing on behalf of my parents, [redacted], who were scammed today by this company. My mother received a pop-up takeover on her computer claiming that it needed technical assistance and to call the "Windows Technical Assistance" number. She did. Then proceeded to let the company access her computer and scan her files. They were on the phone with her for an hour. I have asked her to take her computer to Best Buy tomorrow to ensure it is wiped clean. However, I am worried that they were able to scan and take sensitive information, tax documents, etc. that lived on her drive. She did have the wherewithal to take photos of the things that were happening on her computer, which is how I am sure they hacked in. I am not sure what they did or took or installed. I hope that she and my dad's information is safe, but want to ensure it is reported just in case there's anything this logging of the issue can do. Thank you in advance for your time.
318	98476869	1/29/2018	Block Island, RI	NTS IT Care solicited unneeded services.They tried to get a statement of customer satisfaction. I refused. They took $199.99 from my bank account.NTS solicited business with a banner ad saying they would shut down my computer due to a security breach if I did not call them immediately. This is a scare tactic. They insisted on installing an AdBlock that I did not need, to prevent further banners of that sort. I allowed them to do so, as they had frightened me with their demand that I call them. The process was intrusive and time-wasting, involving their access to my computer. After the installation, they tried to extract a statement of customer satisfaction from me, assuring me that NO money would leave my bank account until they had that statement from me. I refused, I was very angry that point, and I hung up on them. This was in November 2017. The following month, on December 11, 2017, they removed $199.99 from my account. I had given them my debit card number and agreed to a 2-year contract because they frightened me into it by taking control of my computer. — Additional Comments: I went to the NTS IT Care website today, and discovered that the company will give a refund if customer satisfaction is lacking. I hereby demand a refund from this company. As far as I am concerned, they are scam artists who use deception and intimidation to extract money from the unwary.
319	92242707	1/30/2018	Clinton, MD	Consumer is calling stating that he has been receiving phone calls from someone stating to be from NTS. Consumer states that they told him that his computer is emitting a virus. Consumer states that they wanted remote access to his computer. Consumer did provide access.
320	92142175	1/31/2018	Racine, WI	Consumer states that he received a call from someone representing NTS Computer Support stating they have a refund for the consumer of $269.99 because their IT support was being shut down. Consumer was told that he needed to grant remote access to his computer so that he can fill out a refund form. Consumer didn't grant remote access to his computer and kept on asking questions about the refund. Consumer previously paid the same group of individuals but at the time did get his money back. Caller ID info was blocked. UPDATE: 1/31/18 Consumer called to add additional information. [redacted]
321	92330610	2/1/2018	Hale, MI	On the dates i submitted i paid two companies which i think are one and the same i paid in total $499.00 for virus removal andinstalling of firewalls and security cleaners, but now i've got a e-mail saying that the federal trade commision has money for me because they have busted this hackers and that i was hacked. but the spelling and language of the letter is suspect and i feel may be more fishing/ hacking scam. if you could please help me in this matter it would be appreciated. [redacted]

322	98387987	2/1/2018	Florida Gulf Coast University, FL	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 25FAC94E-20B9-49A6-9692-CA6E2656B637. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- could not get out of the page and it keep saying that if you closed closed the computer I would loose everything. call the number listed for microsoft as I understood it. they would clean up the computer and put in norton to protect it from further problems. --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: true --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: Over65
323	98476783	2/9/2018	Omaha, NE	This company tried to scam me buy saying that they wanted to refund my 2 year subscription for service.In January of 2018 I purchased a 2 year program to maintain my computer. Within a month I received a call saying that they wanted to refund my subscription. As I called the person I spoke with was calling from Miami and then he had me ta k to a person in New York. As the person proceeded to try to put the money back on my credit card he said he couldn't do it that way and began to ask me if I had other credit cards. I caught on that he was trying to extort money. And I am wondering how did they know I bought a subscription? I called the place in Miami and they said they where NTS global and the company in California was local. And they said the person in New York wanted to give me money back. Then I called the NTS company in CA and related this and they said this other place is a fraud. But how did this other place find out about my subscription? I am taking a loss of 250.00 and I will not deal with this company. I just want people to know that NTS IT CARE is not a place of integrity. I noticed when the person worked on my computer from NTS in California he took an awful long time. Did he get information and relay to the person who tried to scam me. This all sounds very suspicious of people trying to extort. I would never want to have this company work on my computer remotely. --- Additional Comments: I am seeking no resolution. I am never going to do business with them.
324	92719749	2/13/2018	Omaha, NE	SCAM On December 18, 2017 I paid $54.99 to NTS-IT-CARE, 1605 S. Main St. #125, Milipitas California 95035-6270, 877-490-6709. They flashed a Red Alert sign on my computer saying I had a virus and I fell for it and called them to clean my computer.On January 27, 2018 my computer began to have problems and I called them to take care of it. They roped me into a two-year subscription for $250 to fix my computer on going. Again, I fell for this and they fixed my computer and it seemed OK. On February 5th I received a phone call from a place in Miami, though I was unaware that the call was from there, and they called from this number: 1-786-749-5469 saying they wanted to refund my subscription. They then connected me with another person who was in New York, though I was unaware of this, his name was Eric and he called from: 1-315-504-5508. I went to my computer as I was speaking with Eric and he put up a form on my screen that I was to fill out with my credit card number which I paid the 2-year subscription with. As I proceeded to do this he said he could put it back on my other credit card and he asked me for that card which was a chase bank card. Again I fell for all this not aware that it was a scam going on. I logged onto my Chase account and he put up some numbers on my bank balance and he said he made a mistake That was $2500 too much. He tried to fix it again and he put on an extra $5000. He said he made a mistake again and that he would lose his job. He asked me if I was an honest man and I said I was. I couldn't see that he was scamming me and I fell for it. He said there was a way we could fix it. He asked if I had a Best Buy store nearby and I said I did. Yes me to drive to the Best Buy and get two gift cards one for 100 for 2000 and then to scrape off the back of them and give him the numbers and I did so. I couldn't see this was a scam and it simply happened. After this he had me drive to Walmart and get 9-$500 gift cards and scrap off the back and give him the numbers which I did. The next morning I realized I had been scammed of $6700 and I was devastated.I spoke with synchrony bank today, February 13, 2018 and they said things don't look good because it's not fraud and it was a scam.I also called the number in Miami today (2-13-2018) +1-786-749-5469 and when the man answered I said is this NTS care and he said yes. I then hung up. I also called Eric at +1-315-504-5508, the man who scammed me out of $6700, and I asked his name and he replied Eric and I said I wanted to speak to him about getting a refund on my computer subscription. He asked me my name and I hung up.This is all the details that led up to the scam.
325	92842051	2/17/2018	Flagstaff, AZ	Glenn Richards who previous texted to you would also fix our our I Tablets .
326	92842026	2/17/2018	Flagstaff, AZ	Pop-up. REd and White. It said any futher use on my computer can result in a virus. affecting, on-line banking/purchases, hard drive, e-mail address, and other sther things on my computer, I don't remember exactly.It said to dial 844-208-2608. The rep I talked to is Glenn Richards ext 303. I allowed him access to my computer via-net to fix the problems. and he wanted $249.99 for a one year contract. or 369.99 for a three year contract. He didn't say anything about what the contract involves. I told him I can't pay any I only have $100.00. he went go to talk to the security people and he dropped the price to 89.99 +9.99 for the tech support or phone call. I don't remeber. He wanted me to pay the 89.99 Since I said I have said Ihave 100 and to pay. I told I can;t do that I need thec money for groceriies, gas and other neccities and said I can pay $20.00. and 10.00 a month a month automatic withdrawal on the 16th of every month.Theoriginal was $20.00 a month and $10.00 a month. I was transferred to banking a lady in banking and said I have to pay 25.00 and $15 a month no less. demanding that. I said ok. And I was contacted e-mail by jerry who wanted to text to jerry about something, survey or something else I dobn't remember. I didn't respond.

327	98370313	2/26/2018	Escanaba, MI	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted] m. It will help if you provide the Microsoft reference number EEF7AFF5-252B-4092-9F54-2CFD1A476B95. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- They claim to fix what issue I was supposively having but looking online after the fact I see that company has scammed lots of people.. --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue --- Consumer Age Range: 26-49
328	98394345	2/28/2018	Woburn, MA	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 005502BB-A405-4130-BD59-3A06B04B35A6. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: true --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue --- Consumer Age Range: 26-49
329	98476781	3/1/2018	Bay Saint Louis, MS	Exactly what all other complaints about a pop up then bullied me into a $99.99 charge to clean my computer. I found out my Windows were up to date sSee all other complaints. I called bank and blocked charge. --- Additional Comments: Make sure they do not charge me. When they started working on my computer I got on my iPad and saw these claims and closed my laptop so they could not do any harm.
330	98388395	3/6/2018	Cincinnati, OH	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 72242F06-17E0-497B-A5E3-862ACAEA9F82. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- Computer froze. Alarm indicating potential unprotected status. Agents told me they were certified Microsoft technicians showed me my computer files had been corrupted and offered to fix everything for $249.99. I told them it was too much for me. They lowered it to $169.99. After being shamed for my reluctance to go forward I paid and then found not to be Microsoft. but NTS IC CARE. --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: true --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue --- Consumer Age Range: Over65
331	98388191	3/9/2018	Chicago	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number F1AE3C59-37F5-48D0-9B6D-E898B501C02C. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- I received a popup msg that my computer had been invaded by a virus. In the popup Microsoft was referred and I was instructed to call 833 225 7743 to get assistance. Had long conversation with Woodrow Parker (who had a very thick Indian accent) who explained that to fix the problem NTSI representing Microsof would have to clean out over 11 000 error problems. I allowed them access. Big mistake. --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue
332	94989187	3/9/2018	OH	report only wanted to report NTS-IT Care who scammed her out of $400, SHE had already taken appropriate steps but wanted to give us the name of the scammer --- AARP Type of Complaint: Scam/Financial Exploitation
333	98392272	3/13/2018	Conway, SC	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 6770155B-F521-431D-AF05-E756B1590914. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue --- Consumer Age Range: Over65

334	93694136	3/14/2018	Lakeview, MI	On FB I clicked on a video and a popup showed up saying I had been hacked/had malware, to call immediately or my computer would be locked. When I called he told me his name and when I asked him the name of the company he told me MicroSoft so I continuted to work with them. They accessed remotely-said my network protection had expired and with payment they could put the protection on and get rid of malware. They began to get pushy about paymet and when I asked questions they became frustrated with me. I ended my call telling them I needed to contact my credit card and they called me back twice. I shut down my computer to get them off remote access. They called back from number 424-217-5156.TOPIC:Referrals
335	93614714	3/14/2018	Tucson, AZ	MAIL: The consumer's letter was forwarded by Office of the Arizona Attorney General. Consumer reported going online for HP support and called. The caller claimed that her computer had problems and transferred her to someone who could help. Consumer told the caller she would call back. While the consumer was online she received an alert indicating her computer was infected and to call a number. Consumer noticed that they were the same people and know knows that this was a scam.
336	98476785	3/15/2018	Pleasant Grove, UT	On March15, 2017 I purchased an online service through NTS IT. The service was to provide computer support for 5 years. When the company went bankrupt, I was sent an email, instructing how I could receive a full refund ($299.99). Because I was not able to provide an on-line banking interface for them, I was told that I could NOT receive any refund.I spoke with Ryan Wilson (which I suspect was an alias because he caught himself using a different name from the beginning of the conversation to the end of the conversation). Employee ID: NTSCARE0923. --- Additional Comments: DesiredSettlementID: Other (requires explanation)I realize that this was a scam but would like this business shut down.
337	93594298	3/15/2018	Negaunee, MI	pop up came onto my computer saying My computer was compromised and I needed to call an 800 number. they "sold" me a fix for my computer and charged me $249. My daughter called the company to get my money back as she recognized this as something I did not need and a possible scam. after speaking with 3 different people was unable to get the full amount back and the amount they said they would credit back wont happen for 45 days. The company called her cell phone on 3/15/18 telling her that her computer was being monitored and appeared to be being hacked, however she doesnt have a computer. she recognized the company and asked if it was my computer as they should not be monitoring it any longer because we cancelled the service. They were belligerent to her when she explained to them the situation hanging up and putting her on hold several times. She was told by an operator named "Jack" that he would put his dick in her mouth and in the mouth of her daughter. Finally she called the original number back and spoke with Austin and Allan re; the refund as this company was clearly not on the up and up, he assured her the people she had spoken to that were so verbally nasty to her were NOT from NTS and confirmed that they were refunding her partially but my daughter told them she didnt believe him and was skeptical of the refund. she did call the original number that called her back and asked for Allan, low and behold Allan answered confirming that the operators were indeed all fron NTS. She confronted Allan with this information and he hung up on her. please stop these people, they are helping no one and treating people who are fighting back like hell.
338	98392623	3/15/2018	Mount Pleasant, MI	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 42D08B89-D89C-4EFD-9D49-9EFF7CCCD77A. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- 3/14/18On FB I clicked to listen to a singer/video. Then I got a popup saying my computer was hacked or had malware-was loud gave a code and message to call immediately or my computer would be locked. When I called they remotely started working on my computer told me my network system protection had expired they could get rid of malware start the protection as soon as payment was recd --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue --- Consumer Age Range: Over65
339	93790358	3/20/2018	Brownwood, TX	they somehpw started my computer to scream. and told me not to turn it off or all would be lost. i paid them for a one time fix of 49.00 with a credit card.the phone # they gave me to call if i had any problems 1 844-208-2608.my email address they have and my credit card #TOPIC:Referrals

340	94110010	3/31/2018	Plattsburgh, NY	I had a warning come up on my personal computer stating that I needed to call 844-208-2608 immediately and that my personal information including bank accouts, credit cards, etc. was not protected. I couldn't get past this "warning" that so said all my information on my computer would lost if I didnt call the phone number within the next 5 minutes. There was also a voice recording that kept repeating this warning that I must call. When I called they said they work with Microsoft and when I gave them the error code 268D3 they told me that they don't usually here of this "major corruption from callers. My problem needed major work". They said I had been using Macafee virus protection and that it had ran out 46 days ago. I told him that I didn't use that company for anti-virus and I used Avast free virus proctection. He said the Macafee probably came with the computer and expired (I disagreed) but he went on to say that a "free anti-virus" WOULD NOT PROTECT AGAINST THIS TYPE OF CORRUPTION. He went on to say the only way to fix this would be for me to purchase Macafee Total Protection costing approx $180.00 for 1 year or the best option and savings would be the 3 year total protection for $430.00. When I said that was VERY expensive and asked why? He went on to say that purchasing this would be my only option of fixing this major corruption after showing me on my screen (he had control of my cursor) all of my "corrupt files". He asked which option I would be purchasing, I told him that I could only afford the 1 year plan. He was presuring me to uy the 3 year plan. I told him the price was too much. He asked if I was a "senior"? I replied that I'm in my 50's. He put me on hold to "talk with his supervisor to see about a discount." He came back to say he had a very good deal for me. They would offer the 3 year protection for 349.99 + tax. I felt very pressured and he said the 3 year was much better protection than the 1 year. I agreed although I all along was questioning whether this was legitimate. He kept saying that NTS works directly with Microsoft and had me print out I of the services they provide. I went ahead and said "ok" to the 3 year purchase (after being tied up for 1 hour on the phone speaking with 3 different people at the company vying how good their company is. When entering my credit card payment info, they took over the signing of my name! They did an electronic signature not even asking my permission to do so! He claimed this is the only way to authorize the purchase. I then had to stay at home near my computer for "Harry" to call me when it was all fixed. It appears to be working ok now, although I have Googled the NTS IT CARE company (now that I can use my computer) and there were multiple hits that this company is a SCAM! I am very upset at myself for falling for this and will be filing a complaint regarding the charge with my credit card. I can see now how awful it feels to be scammed. I want to know how and why NTS can do this. How come they are still in operation? They were hard to understand with heavy accents (from India?). Terrible they are preying on people!
341	94135548	4/1/2018	Newton, IL	Was on the computer and got a message that it would be shut down if I did'nt call the number to have virus fixed. Had to or it would effect entire network I was on.
342	97578264	4/3/2018	New York, NY	These guys are scammers they send pop up on your computers and charge money for fake support. IsVictim:true --- Initial Means of Contact: Unknown
343	94313910	4/4/2018	Broomall, PA	I was awaiting confirmation of package from UPS/Fed Ex when I rec'd pop up on my computer/e-mail FED EX tracking #-When I opened up rec'd notice that I now had a virus and that I needed to call 1-844-208-2608 number to speak to authorized rep to clean up the virus or my system/programs would be should down and everything corrupted. I called the number and spoke first to Woodrow(Indian accent) who advised he could make it all right and promoted a $199. annual charge or a 3 year service/support monitor for $399.99 and based on his review I could cancel Norton & Malware charges at renewal -thus saving money.He would get right to work-but needed me to speak to their payment person .Provided credit card info and had to speak to Citi card rep as they did not initially authorize as this was not my "normal way" of doing tranactions. I asked Citi Rep about Company(NTS IT Care) and [redacted] had no knowledge of organization/good or bad. Thus -I ok'd payment and Woodrow then Harry new rep"fixed" my computer and placed their info on the system. I'm unsure if anything was really done accept they -took off their FEDEX e-mail notification and processed a credit chard charge for $399.99 for service that I doubt I'll have available . I definetly fell for the scam and now wonder if I need to take my computer for a legit clean up. I have cancelled my credit card just as as precaution. Looking for next steps and appreciate any input that you can offer.
344	94343613	4/5/2018	Leavenworth, KS	Consumer states that while she was on her computer she received a pop of warning the consumer of that a pornographic site took over her computer. Consumer was instructed to call Microsoft which she called, granted the caller remote access to his computer. Consumer paid $199.98 via her CC and the company that made the charge was IT Care and since her Web route has been shut off.
345	98400016	4/8/2018	Leavenworth, KS	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number EAFAA4B7-2DFF-4841-8B02-309399B58AF0. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- On April 2 I was trying to get into my e-mail and couldnt. I closed out and went to the Outlook web site. The minute I clicked on to the site a pop up came up with the Microsoft logo on it that said that my computer had been compromised by a pornographic site and they could be steeling personal information from your bank accounts credit cards ect. It said that I shouldnt shut down my computer. --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: false --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: 50-65

346	94478895	4/10/2018	Corona, CA	The consumer reports someone from the company NTS contacted her. They stated she was owed a $200 refund for computer work that was done. The consumer reports they asked for her debit card information. The consumer reports she gave them the information. The consumer reports they put $2000 into her checking account. The consumer reports that they took the funds off her credit card and put it into her checking account. They wanted her to send the left over money through gift cards. The consumer reports she didn't send them any money.
347	98364521	4/11/2018	Fountain Valley, CA	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 42EBFAEA-2D2A-4099-88DE-71807A49BE5F. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- I suddenly had a huge popup with MS Windows Logo saying I needed to contact this number and if I didnt my computer WOULD be damaged (not MIGHT). I could not close or minimize screen and had to reboot to close! I called 2x and spke to men who both wanted immediate access to my computer. I refused each both & upset both techs This was very upsetting and scary with the popup and bullying!!!! --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: true --- Fraudulent Person Access Computer Remotely: false --- Remote Access Software Name: LogMeInOrLogMeInRescue --- Consumer Age Range: 50-65
348	97580216	4/17/2018	Pittsburgh, PA	On April 17, 2018 while on Facebook, I clicked on a picture and warning messages appeared stating my computer was infected with viruses and would shut down. I panicked and believed my computer was under immediate attack, and persuaded that NTS IT Care was an authorized agent for Microsoft. I was told my computer was infected with numerous viruses, and offered recovery services for $***** which I paid. Once paid, it appeared they were doing something in my computer then a message that it was fixed and to call them even though I had given them my number to call me. The representative named Eric said this one time fix was guaranteed for 7 days and that it would be fixed for no additional charge if something happened to my computer. The representative tried to get me to purchase internet protection and said I would no longer need McAfee. I was very suspicious of this entire ordeal. I will see what happens after this 7 days is up. Hopefully nothing more happens to my computer. The computer does seem a little different now - it blackens out which didn't happen before - like it's being monitored. IsVictim:true --- Initial Means of Contact: Unknown
349	100319662	4/18/2018	Madison, WI	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number CEB9F6EF-948C-4325-8A7C-C5125C3E15E3. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- the hackers. access my computer. also made it seem like I could not use my computer until I brought there services. --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: Other --- Other Software Name: micorosolt
350	98364054	4/24/2018	West Suffield, CT	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 7D51D5D7-696B-4747-92D1-C33A95962710. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- Pop up said my computer was having major Microsoft issues and I could not turn it off or my computer would crash. Had a number I was to call in order to fix the problem. Enclosed video from you tube which describes my same experience with them.https://www.stopphonescammers.com/2017/10/11/nts-care-tech-support-scam-fake-pop-scammers/ --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: 50-65

351	94898824	4/24/2018	Westphalia, KS	A big warning sign appeared on my computer just as I was about to open a post on Facebook. A recorded message began to play and the information both on the screen and the audio told me that I must call this number in order that my data would not be hacked into and lost. The number they gave me was 844-208-2608. The technicians name was Alex and I was so panicked I wasnt thinking straight or I would have known this was a scam. I ended up giving them my debit card number after they showed me on the screen how many error messages I had ignored over the course of two years and circled in red the virus cleaner company I had on an icon that they said was fake. They removed it. Also I had something called "Ask" on my screen that was always there and they said that I shouldnt use that. I think they took it off. too. They told me how I should be backing up all my info periodically and that they would do that for me from now on. This led into the cost of their services which he said would be 199, but when he found out i was a senior he gave me the senior discount. He made a receipt on my notepad and printed it out on my computer. Like an idiot I gave him my password to my computer. He was already into it anyway with complete control of my mouse. They said to call them every month so they could update my computer/files. I asked them if they were going to keep away the scammers and the viruses and thaey said Of course we will. Now I am ready to just cancel my internet with Dish, I am so paranoid. I did get the bank on the phone afterwards and there is a hold on my Debit card they used. They told me they would fix everything and call me back which they did. They also put their icon on my startup screen so maybe you can use this clue. I will not be checking email too often, but I will wait for you to respond and if I can help in any way to catch these thieves let me know.
352	98403400	4/24/2018	Houston, TX	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] a [redacted]. It will help if you provide the Microsoft reference number AD791F0E-F787-412A-9C24-D76AAA17F88A. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- This company has contact me by email several times. I delete the emails. --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue --- Consumer Age Range: Over65
353	96961216	4/25/2018	Greensboro, NC	NTS IT Care creates a pop up indicating a virus on your pc which directs you to call them. Afterwhich, you are pressured into purchasing tech service.I was on my brand new pc and went to microsoft edge search and was in my newsfeed page when a pop up indicated my pc was infected with a virus and locked up my pc. I was immediatedly directed to call NTS IT Care at phone number 1-877-???-????, 1605 S. Main St, Ste 125 Milipitas, CA 95035. I can't recall the last 7 digits of the ph# because it conveniently a different ph# 844-208-2608 is provided once they used high pressure sales tactics to show me how my pc was allegedly infected and how I needed to purchase once of their tech service plans in order to avoid this from happening in the future. I asked if my pc was going to be repaired right then since I was locked out of it and rep/Jack indicated yes but continued to pursue the issue that I needed to purchase the tech service plan to avoid this issue in the future. Rep/Jack proceeded to ask which plan I wanted; 1 year for 139.99 or 2 year for 199.99 or a 3 year plan for 299.99? He could tell I was hesitant; so he began to show me the alleged issued on my pc via having remoted into my system. He could further tell I was hesitant as he asked me all these questions about my pc use such as if I paid bills online or made purchases online or had any social media accounts; which according to him were now at great risk. I informed him I don't do online banking, I don't make online purchased from my pc and I don't use social media nor do I want any of those types of accounts. Because, I am not tech savvy and my pc is locked up at this point; he convincingly shows me some file that he stated were harmful to my pc and had been added as a result of me surfing the internet. Jack asked which plan I wanted to purchase to resolve and protect me from future issues. I indicated the 1 year plan for $139.99; at which time he transferred me to the billing department, after having me provided my personal information to include my visa credit card number. I was placed on hold for approval of the payment. Transferred back to Jack; and advised a tech would begin the process of repairing my pc from the viruses via remote.Jack additionally advised I was being sent an email confirmation and receipt for the for the 1 year service plan which I printed. The tech who worked on my pc was named Austin. I watched my pc as he worked via remote to alter and allegedly repair things on my pc. While, tech Austin was doing this, I searched for NTS IT Care via my tablet. I found them on the BBB and saw there were 48 complaints filed against this company alleging scams. Unfortunately, they'd already charged my credit card but I do plan to follow up with my bank and try to stop the payment. Tech Austin speaks with me upon completing the alleged needed repairs and ask me to complete a feedback request reference his assistance via email. I did so but was very clear in the feedback request that I had been very uncomfortable throughout the entire process and advised I had looked up their company online through BBB and found they had a lot of negative complaints against their company. I further informed him I found it odd that when this alleged virus pops up the pc owner is immediately directed to their company at the 1-877-rest unknown number. Tech Austin attempted to explain the number defaults to whatever tech company is available at that moment to assist the customer, which did not sound plaus ble to me. I was then transferred to someone named George (Owner/Head of Customer Service) who tried to reassure me someone from NTS would contact me tomorrow to make sure my pc was still working fine. He asked if I had any other questions for him to which I stated no; since I planned to do my own follow up reference this matter. --- Additional Comments: I want this business to stop utilizing this hijacking method of creating this pop-up which gives the impression your pc has been leg

354	96065891	4/25/2018	Windsor Locks, CT	Scam Artists. Froze my computer and used Microsoft name saying my computer could not be shut down. Supplied there telephone number not Microsoft. This all happened April 5, 2018They froze my computer and informed me my computer would crash if I shut it down. They supplied a telephone number and instructed me to call to resolve issue with my computer. I called and they immediately said they were going to go into my system to fix the problem. I gave them access like a fool believing they were like Microsoft fixing my system. They had a script they used to inform me that I had a Trojan virus. I am enclosing a you-tube link which is the exact same script they threw at me.https://www.stopphonescammers.com/2017/10/11/nts-care-tech-support-scam-fake-pop-scammers/ They kept trying to sell me 1 year and/or 3 year for repairing my computer. I was in panic mode and told them I could only afford the 1 year plan. They kept transferring me different people who kept hammering at me to purchase the more expensive plan. I kept asking them why the sales pitch??Why isn't someone fixing my system which is locked. They told me that once they got the money from me they would fix the system which should take about 30+ minutes. Stupid me gave them the $149.99 and then they said the guy who was going to fix it needed $20.00 from me to bring it up to $169.99. They didn't send me to a secure platform for the payment. They just had me type out my card number, expiration date, and security code. Boy was I an idiot! The guy (Victor) says he fixed it. Took less then a minute not 30 minutes and then asked me to go into my E-Mail to see if it worked. While I was in e-mail he took over the system and composed an e-mail to ntsitcare which said I [redacted]) had no further issues with the computer and that it was working fine now and signed my name and sent it. When I got off the phone with them I immediately googles the company and was made aware that I had been scammed. I called my bank Chase within 15 minutes of hanging up the phone. Told them to cancel the payment and had Chase cancel my card and issue me a new card. April Now I am telling them that I have the Better Business Bureau saying that this company is a scam, however, they are telling me that if I look to the right of the screen they have a lot of good reviews. I told them that anybody can right good reviews especially there company employees and people they pay off to right good reviews. They sent me e-mails saying to call them on April 20 and 22. I responded back that I wanted my card credited. They will not put anything in writing. They just keep telling me to call which I do April 20-23 and will not tell me that I am getting refunded. This last call I told them to stop calling me and just issue me my money back. He insisted I at least pay for repair work done to computer on April 5, 2018. I told him there was nothing wrong with my computer to begin with. I have Norton anti-virus and they are the ones who froze my computer to get me to call them. --- Additional Comments: I want a credit to my credit card for $169.99 which they charged me and is in dispute at this time with the bank. I want no further contact from them after the credit is issued.
355	95117130	4/27/2018	Chicago, IL	I thought virus alert came from Microsoft. To get rid of the alert, I let "tech" person take over my computer and take my credit card number. Turned out a third party was doing this, not Microsoft. later saw many scam complaints re NTS IT CARE on Google.TOPIC:Referrals UPDATE 4-27-2018 Consumer is calling back to see what he has to do. He was given a general guidance. [redacted]
356	95190559	5/1/2018	Del Rio, TX	Consumer states that he got a pop up on his computer and he called NTS Computer Systems and gave them remote access to his computer. He states that he now got a call from them telling him that he had a virus and he had to pay them $300 via Google Play cards. He later realized it was a scam when they asked him for more money.
357	97583385	5/8/2018	Saint Paul, MN	I was on facebook Friday April 20, 2018 And all the saddened they hacked my computer and I could not get them off unless I called the number on the screen, Which like a dummie I did. I asked them immed. if the were affiliated with Microsoft and the said yes. In fact I asked them 2-3 times and got the same answer. So a person by the name of Harry, started taking all my security and ad blockers and every thing I had on my computer off and put all of theirs on it. So I asked them out much am I going to be charge for this, which he said he'd tell me in a minute. I have never had any of this happen to me before so I had know idea what was going on. So to the tune of $428.28 but at the end this lady came on and said, do not call anyone but us for your computer or printer problem they were independent and not affiliated with Microsoft. Which I was running late for work and didn't have and time left and they had my money and the computer was running okay. So I would talk to the in the morning. I contacted my bank who is dealing with them now. But I wanted you people to know what they are doing and hope no one else get taken.. Plus their reviews are not very good and they have told other people the are working with Microsoft. They even put there whole phone number on my Screen at the bottom. I have had Microsoft take every thing off they put on and now I am up and running like It should. I did receive a letter in the mail from you, but this was easier to fill out. IsVictim:true --- Initial Means of Contact: Unknown
358	97584037	5/12/2018	Milledgeville, GA	Multiple Popup windows filled screen and denied ability to close windows; continued popup windows claiming errors and appearing as attack; the windows listed this phone number to call to remove and person called 844-208-2608. Once on phone 'support person' claimed among other things when customer noted that Norton should have caught this that antivirus was not installed and given access to computer by remote was then able to install software to repair and now that software is loaded and NTS with phone number is loaded onto multiple places in screen. Company convinced caller that they could repair computer, via remote access loaded NTS software and charged card $******. Following this crisis event, caller realized that this was an event seeming to be created by NTS to then draw in the 'customer' for them to then charge and serve. Have filed dispute and also file this complaint. IsVictim:false --- Initial Means of Contact: Unknown

359	95695364	5/15/2018	-	there was a popup on my screen shwing that my computer is locked and I need to call microsoft tech support by phone number 8772219222 and my computer Was completely locked I couldn't access to any other websites so I called them there was an Indian accent lady and she told me that OK tell me the error code or what were you doing while this happened.what is the internet provider. Then I got suspicious and I hung up she called me back again but they said I need I will get back to you later but I couldn't fix the problem and my computer was locked so I called them again this time there was a guy but again with an Indian English accent I told him what was the problems he also asked me some of these routine questions finally he told me that I need to have access to your computer remotely to figure out what is the actual problem so he gave me The code and I entered it. He had access to my computer for about 5 to 10 minutes and I could see what he was doing but actually I don't know if he was able to do something that I'm not aware of like a stealing data from my computer. So then we end he told me that OK there are some viruses on your computer and you need to get antivirus I said OK is it for free or notAnd he said no you have to pay 69.99 for fixing your computer and the removing the junk and all of those stuff and he wanted to ask me for a billing information and the card numberAt that moment and I told him that I need to consult with my husband and get back to you and I hung up and then when I ask my husband he was like it wasn't a scam and why did you let them have a remote access to your computer. so I am just so upset I don't know what to do. I put all the information that I have about their company and their phone number that I contacted and the email address so I don't know if it works you can just catch them.
360	95807780	5/18/2018	Spicer, MN	Consumer received a pop up message on her computer from NTS Help Desk Inc stating that her device was being hacked and gave a number for her to call for technical assistance. She called and allowed them to gain remote access to her computer. They asked for her bank account info to charge their service fee of $359.99. This also covered protection software. She discovered that they actually charged $156k.
361	95854657	5/21/2018	Saint Louis, MO	My father has IT service through NTS IT Care. Last week, he received several pop-ups saying his computer had a virus. He then received a phone call from a person name Dave who claimed to work for NTS saying he know my father's computer was infected and he needed to remote in. He set up an appointment on Saturday with him over the phone and told him he needed to purchase $2200 of Google Play gift cards. These were needed to purchase the google software needed to clean his computer from the virus. He told my father a technician would be coming to his office on Tuesday to swap out the computer. At the time, my dad would receive the rebate for the $2200. He had my dad read the activation number on the cards and then told him that none of them went through and to go purchase more. My dad did not but Dave said he would call back on Monday so he could. At this point, my dad tells me and I immediately call NTS and confirm this person does not work for them. I called Dave and he tried to convince me that I wasn't speaking to NTS when I called and he was real and then gave me a fake Microsoft IT support number. He gave me the number of the technician who I called. Same story - lied and told me NTS was lying to me. I have the google play activation codes (all which had been redeemed) and the phone numbers (one of which is was a google voice number).Dave (760)933-9388Robert (309) 791-4140Fake IT support 1-888-807-5084Google play activation codes5U5G J65C 117P C61D R122727U AME7 UF64 Q70X 8TMD9Q40 LWEO K3SU KCNW QMYB8RS1 G7SC RGNQ LAKB UC1342CJ 9G4Z YSOR 35NZ KJYN
362	98380806	5/22/2018	Eagan	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 34A93E6C-15B8-4BAB-B9C1-495224FFBA4F. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- I was online checking my my account and a pop up message stated that there were Microsoft updates that needed to be installed and to click update to install them. I did that and then I got a phone call from a man that said my computer had viruses and someone was trying to get into my accounts. He said he had worked with me in the past. --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow
363	96173579	5/23/2018	Saint Paul, MN	April 20th I was on my computer on Facebook and all the sudden a virus came across my computer screen which I could not get off unless I called this number on my screen and it was NTS itcare at 866-763-1760. Which I asked them many times if they were affiliated with Microsoft and they said yes, until the end after they took all of my security, adblocker and every thing I had on my computer and put there own stuff on my computer. then they told me how much it would be for 3 years protection. So I paid with my debit card $428.28. That's when the said after they got my money, they were not affiliated with anyone they were independent. Well I have to hang up to leave for work. And I couldn't do anything until Monday April 22, 2018. My bank said they got the money so they are working with me to get it back, and I did reach out to Microsoft and they took every thing off they put on my computer and put the security etc on. I just wanted to post this so no one else has to deal with these under handed people. They have many complaints on them in the BBB in Los Angles, CaProduct_Or_Service: Computer --- Additional Comments: DesiredSettlementID: Other (requires explanation)Just wish the business wouldn't put the viruses on people PC's. Scared the crap right out of me. Never had that before.Just want the BBB, to make note if any one wants to use them. They are not honest
364	96086257	5/25/2018	Charlotte, NC	This company infected my mom's computer w/virus, then gave her a number to call to fix it: 1-844-208-2608. Network Technical System. She gave them her credit card info & they charged her $249. My mom suffers from dementia and this is the second time this has happened to her! UPDATED: 5/25/2018 The consumer called to ask about her complaint. [redacted]

365	97124824	5/29/2018	Wheat Ridge, CO	They hacked my computer and told me I had a virus on it. In order to get control of my computer I had to pay them 270.00. I was forced to pay.They hacked into my computer and froze the page saying that Microsoft had authorized them to fix my computer because it would ruin them if I didn't. The message was left on for most of the conversation. Then they gained control of my computer and showed me thousands of WARNINGS on it that had to be cleared. They promised to fix it but they took me to a page with their prices on it. I asked them if microsoft would fix it if I didn't take the protection. They avoided the answer until I gave up. They took my credit card information and gave me a 30.00 dollar discount for being old. Then they left their phone number for any problems. Here is what I found on their web site.NTS IT Care Inc. is an Independent Service Provider and is NOT associated or affiliated with any other Brand(Microsoft/Windows/Apple) or Internet Service Provider.SO THE WHOLE THING IS A SCAM AND i WANT MY MONEY BACK! $370.00 --- Additional Comments: i WANT ASSURANCES THEY WILL STAY OUT OF MY COMPUTER AND THEY WILL NOT DO THAT TO ANYONE ELSE.
366	97586542	5/30/2018	South River, NJ	My mother received an email and when she opened it her whole computer froze. A number showed up for her to call. She called and was told that her computer was hacked and got her to share her screen with the person on the phone who said he was named Ryan. He then told her they can have a technician fix it, but it would cost $**. My mom then told him she would have her son look at it. Ryan told her that he wouldn't be able to fix this, which made my mom suspicious, so she told him that her son is a computer programmer so yes he would know and then she hung up. I am currently running a scan using Norton hoping that this scammer didn't insert any virus on the computer. IsVictim:false --- Initial Means of Contact: Unknown
367	87527529	5/31/2018	Surprise, AZ	MAIL: Forwarded by the Office of the Arizona Attorney General -The consumer reports the following: computer scam - pop-up came on freezing the computer- pop-up indicated it was a Microsoft support and with an additional pop-up said to call 866-763-1760 to unfreeze computer. I called Microsoft support and they verified this was a scam"
368	96405802	6/6/2018	Sinclairville, NY	Consumer states that she received a phone call from someone claiming to be with NTS. Stating that something was wrong with her computer and needed access to the computer to fix the problem stating that her computer was infected consumer did grant access.
369	96454574	6/8/2018	San Diego, CA	Consumer is calling to report that she received a notification on her computer stating they needed her to call another number. Consumer called the number and spoke with someone claiming to be with NTS IT Care Inc. stating that they needed her to pay 49.99 dollars in order to fix the problem. Consumer paid through credit card. Consumer received another phone call months later from the same company and was asked for her to get on her computer but she did not continue with the call. UPDATE 06/08/2018 Consumer is calling to report that the same entity called her again [redacted]
370	96547088	6/9/2018	San Antonio, TX	My complaint is the same as other people who have the given the following info to BBB.... PATTERN OF COMPLAINTS"According to BBB files, our records show that the company has a pattern of complaints. Consumers allege receiving a pop up on their computer, which leads them to believe they have a virus. Consumers claim that the company then uses forceful and deceptive sales tactics to remove the virus. Consumers have alleged no virus was found when computers were taken to an alternate third party repair or having to pay $199.99-299.99 to have the "virus" removed On June 16, 2016 the BBB contacted the company in regards to our concerns about the amount and the pattern of complaints we have received. Unfortunately, the BBB did not receive a response. " However in my case, it was $570 over 2 days instead of the $199.99-299.99 as stated in the BBB
371	96171171	6/13/2018	Littleton, CO	Consumer says that his wife was on the computer and it told her to call a certain number of or the computer would crash. The consumer spouse purchased a 3 year contract for $400. The consumer cancelled the contracted within 24 hours, that is the next day cancelled. Consumer says that the Bank of America would not cancel the contract. UPDATE 06/13/2018 MAIL: Forwarded by the Colorado Department of Law. Consumer reports for herself and her husband and adds to the complaint including company name NTS IT Care and representative name. Consumer notes their credit card company has not honored their request to return dispute the charge. [redacted]
372	98913871	6/14/2018	Columbus, OH	NOTE: In addition to the complaint notes immediately below, the Ohio Attorney General's Office provided additional information in fields whose header titles are quoted and follow the complaint notes. --- I want NTS prosecuted to the fullest extent of the law, and I want these scam artists sent to prison. I also want my money back. --- Topic Description: I placed a two-year warranty on my Lenovo laptop with NTS IT Care on December 18, 2017. Paid $ 249 on my debit card then. On June 12, they (NTS) call back, saying that my computer has been hacked by international hackers. They make me go to a nearby Kroger to get $ 400 worth in a Google Play Card. On June 13, they say that they need another $ 1500 in these same cards. It changed to $ 800 when I told them I don't have that kind of money. They made me go back to. Kroger and get two more cards in total of $ 800. Two hours later, they called back saying the keys were not valid. I was furious with them, demanding my money back, and I threatened them with legal action. I knew I was duped. After ta king with friends and family, my worst nightmares were confirmed. I was conned out of nearly $ 1500 by this "company" that I trusted with my laptop, that I worked hard for. I am furious that I have absolutely no computer for any of my day to day usage. I want justice.A detailed report was also filed with the Columbus Division of Police.
373	96129260	6/14/2018	Castle Rock, CO	Consumer reports that he received a Microsoft warning popped put on his computer. Consumer reports that he entered her card information and was fraudulently charged $300. Consumer reports that he called the number and someone has remote access into his computer.

374	94395683	6/18/2018	Clovis, CA	The consumer was online and received a pop up from someone posing as Microsoft asking for a call. The consumer called and they said they were NTS Software Supplement. The suspects requested access to her computer and the consumer complied. The suspects requested 200 via an unknown payment method. The consumer did not comply. UPDATE: 06/18/2018 Consumer calling back about a ring she saw on a Facebook ad for Birthstone Deals [redacted]
375	98834631	6/20/2018	Chesterfield, VA	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number C9EC7419-F616-4B06-8F54-8AA21FF51B89. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- I keep getting pop-up with loud announcement saying my pc is infected & that it will be locked. They also use Microsoft edge logo & Microsoft on pop-up. It happens a lot when edge is browser. Seems I ke they cant get through Firefox Browser. Call this # 1-877-783-9329. They are waiting to scam You --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: true --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue --- Consumer Age Range: Over65
376	98832436	6/29/2018	Cleveland, OH	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number EDDD65DE-57B2-4656-B4AF-AE59284DF16E. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- got a blue and white screen interrupting my computer with a small gray box in middle with Microsoft name. person sais her represented Microsoft and I needed to pay fifty dollars for him to fix computer I got a phone call on Wednesday from a lady stating same and that my computer would not work unless I called and paid. --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: Over65
377	97341637	7/2/2018	Houston, TX	Recieved call alerting me that my computer was hacked. ID was NTS IT Care which is my security service. Then claimed they needed me to buy Google play cards to enable new security tool using scratch off numbers. This continued over two days as they coerced me to buy $16800. google play cards. Every time I Q them they showed phone numbers to verify. During this period they claimed to be working with the US Govt cyber group. Soon they offered to replace my computor & reimbuse showing check & pic of compurtor as carrot. When they asked for another 4k$ I pulled the plug & cancelled session. Since learned they were imposters & the real NTS restored & secured my laptop. I have tried w/o success to report this to Google. Their system is never talk to customers. Believe they are complicit with this scam. Now learned Google play cards are used for many scams. Hope you can help to shut these criminals down.
378	97459353	7/5/2018	Ebensburg, PA	Consumer received pop up from party claiming to be Microsoft, stating consumer needed to call them about a computer problem. When consumer called she was told that they could install an anti-virus program for $265, which consumer paid by credit card. Consumer no suspects scam. Identity theft steps provided.
379	97629189	7/10/2018	Ebensburg, PA	Consumer is calling to report that she had a computer scam on 07/04/2018 She stated that there was a pop up from the NTS IT CARE company letting her know that they was a technician letting her know that she had to call them back and not to turn off her computer. She did called them back and asked her for her Micro Soft ID number and put her SS number. She was charged the amount of $ 265 dollars from her charge account that she them cancelled.
380	100319471	7/14/2018	Washington, VA	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number BBEA76DF-24DD-4187-8C83-450550916B5B. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- I received a pop-up saying your bank account may have be hacked. Hacked please do not attempt to access your account until you call this 844-484-5482. Then I was asked to provide access to my lap-top to look for Trojan assault on and that Microsoft can provide security software at a basic and advanced level. At that time I asked them to send me the information and would read and decide --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: ShowMyPC --- Consumer Age Range: Under18
381	97760207	7/14/2018	Syracuse, NY	In November my computor locked up saying i was hacked ineededto call them and they would fix it. after awhile my pc was working.I got toll free #tocall and login box from ITSit.never heard from them again until yesterday July13th. that they wanted to let me know that be cause of problems with theresoftware was not working right they wanted to refund the orignal money I paid $199.00 and a free year of service.then they tried to set up paypal to refund my money intead of reading $200.00 it came up$2000.00.In order to fix the amount I had to get$1800 in gift cardsfor them and then threw paypal I would get a full refund of$2000.00 after I get a phone call from them that it was all set.So far I have not gotten a call today. Other-Other Update

382	98828617	7/16/2018	Denver	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number A362A58C-4235-4408-8F2F-D657633C1CDB. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- We got a pop up on our computer.We called the phone number on the pop up.The rep. asked us to clik some buttons. This gave her remote access to the computer with out her telling us that that is what she was doing. She proceeded to entering credit and banking accounts. She said if I can do this so could a hacker and tried to sale us a Synamtec Endpoint Protection subscription for $352.00. --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: true --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow
383	92612050	7/16/2018	Sun City Center, FL	While on my computer, on 11/20/2017 a pop-up appeared on my screen indicating that there was a problem with my computer per Microsoft and to call the number on the screen and not to shut off my computer. It actually wasn't Microsoft, but it was NTS IT CARE Inc (who at the time I believed was acting as an agent for Microsoft - which turned out not to be the case. The person I talked to indicated that my firewall had been breached and that they could "fix it". I found out later through my virus protection provider (Norton) that this wasn't true, and that my computer had not been breached, and Norton conveyed that I had been victimiized by a tech support scam. They suggested that I contact my credit card company to see if they could recover the $249.99 charge (which I attempted too, but without success as of 2/8/18). I also did a search on-line and found examples of others who have experienced similar / and even worse problems. The $249.99 was a one-time charge to "fix" the breach and to provide a two years support with network security for 1 window computer. It was to be my responsibility to contact them once a month over the next two years so they could scan my computer. The more I thought about what had occurred, the more I wasn't comfortable about it. That's when I contacted Norton on 11/26/17 and also did a search on consumer complaints. Based on what happened to me and apparently others - this company appears to be in the business of scamming people - which in my mind is fraud! If there is any way you can be of assistance in recovering the $249.99 that was in my mind stolen from me, I would greatly appreciate it. You can reach me at the e-mail address or phone number I previously provided. UPDATE: 02/22/2018 Consumer calling in because he rcv'd a call from Unknown. They left him a message stating his Microsoft license had expired and needed to call back. Consumer didn't call back. [redacted] UPDATE 07/16/2018: Consumer is calling to report that he received a call from an individual stating to be from NTS IT Care offering a refund. Consumer did not comply . [redacted]
384	97800683	7/16/2018	-	NTS IT CARE INC. contacted me to provide a 2 year firewall extended software warranty. I paid for this care plan. A couple days before today, I got called stating that there was an issue with the software and that i was eligible for a refund. A mistake occurred during the refund process. I was demanded to purchase apple store gift cards. the information on the gift cards were handed out. I called apple and contacted my bank. I believe that Ihave been scammed of my money. Other-Other Update
385	98832178	7/18/2018	Mobile, FL	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 394E8BEF-6B98-4CE0-9DCF-BCED54BD6ABB. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- Our laptop had a red screen and verbal message that kept repeating and was locked. The message had a number to call for Microsoft support. The person told us our IP address had been compromised and our information and identity could be stolen. He offered to fix the problem for $99.99 and suggested we buy network protection from him for $149.99 for one year. --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: false --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: 50-65
386	101845088	7/23/2018	Belmont, CA	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number DF5D76F8-A7EB-4C80-96BB-6EC8DEBE52FC. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- I got a popup window with a line that says Contact Our Certified Windows Technicians for Immediate Assistance +1-844-386-7623. In the bottom corner of the screen is a Microsoft logo with the same message. So I called that number and a man who told me he was technical support and asked me to get access to my laptop so he could fix the problem. I gave him the access and now my laptop is not working --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: 50-65

387	98477810	7/24/2018	Yuma, AZ	I was using my computer when my screen went white and a white pop-up came up saying I needed to call this number in the next 5 minutes because my computer may have been hacked and my banking, credit card, etc. information maybe at risk. This pop up message was being read out loud to me loudly over and over again. I had no longer any icons on my computer screen so I could not log out. I called the number and they said that my Microsoft services on my computer were corrupted. they said I had csr.exe intrusion trojan bugs & 261 spyware in c drive of my computer & malware. They asked what protection I am using on my computer and I said Avira (the free version), which they said does not have enough protection for everything our there). They said I needed McAfee Advanced Protection (it has 3 later protection) and cost is with tax $****** for 1 year. This includes 1 time each month a health check tune up. I need to call them though each month for them to do it. Yesterday I bought our local Yuma newspaper and it had an article in their about fake support numbers scamming people. After reading the article I knew I'd been scammed. I called NTS It Care, Inc. telling them I didn't want their MaAfee and that they are a scam and he said, 'no we are not a scam. We gave you phone number so you can reach us. He had his billing department call me back, but I didn't get anywhere with them either. IsVictim:true --- Initial Means of Contact: Unknown
388	101846391	7/24/2018	Cresbard, SD	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 4F6F9E78-C6E1-4F66-88DC-C05D2AEAF46E. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- i was trying to pay bills on line and the popup came and my computer locked up with a warning that some one was trying to get my bank information and nothing i did would unlock the screen. i could not even shut the laptop off. i called the number and they said that they were a support company or Micro sotf --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: Over65
389	98093605	7/25/2018	Henderson, NV	The consumer filed a complaint against NTS ITCare, because they pressed the consumer into subscripting to a computer service, and the consumer paid them $249.99 on her CC. The consumer latter got a popup on her PC claiming to be from Microsoft there was a issue with her PC. The consumer called them back and they locked the consumer PC.
390	98127761	7/25/2018	North Las Vegas, NV	Consumer reports they received a call from Microsoft requesting access to their computer to update her service. Consumer reports they could not update unless she paid a fee. Consumer complied.
391	98145770	7/26/2018	Oklahoma City, OK	Sadly, i fell for this. i gave them access to my computer. theyve called and ask if ive got into my computer since the date they said they fixed my computer for the next 7 days. NO! of course. Since theyve now called 3 time. In these ldt 2 days they've ordered checks from my bank acct and written around $3000.00. Im so angry at myself. This mistake on my part has cost me so much time. in my case they also were Indian. How do you stop these people?
392	101846429	7/27/2018	Beaverton, OR	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 14CBBF35-27D2-4ECE-8258-A17356D1343C. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- Red pop up on my screen and it had microsoft name on it and NTS IT CARE phone number on it and my computer was locked up called the number and let them in my system thru LogMEin Rescue and they cleaned it i guess my antivirus protection who knows ??? --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue --- Consumer Age Range: 50-65
393	101844389	7/27/2018	White Stone, SC	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number C9AC59CA-F09B-4CC8-9E4E-48D00381EF51. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- Credit Card --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: TeamViewer --- Consumer Age Range: Over65

394	101845180	7/27/2018	Las Vegas, NV	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigato [redacted] a [redacted]. It will help if you provide the Microsoft reference number 0F8D5AEE-85D8-44F0-A7BC-DDEB2BA014D3. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- My computer was frozen and their ad popped up saying to call them right away not to close my computer. When I called they said they work with Microsoft to fix this problem. They installed their software and released my computer back to me. Upon checking with the BBB I learned this was a low risk fraud company.I removed software the next morning. I tried to cancel the charge . --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue --- Consumer Age Range: Over65
395	101846922	8/3/2018	Mechanicsburg, PA	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 0873CEB0-3ED6-41FF-8F8E-D7CD7AAA04A7. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- Had a pop up telling me I had a virus and call 866-763-1760. If I did not do this all my info would be out there and would not ever be available. When I ta ked to sunil Kumar I was told they needed to fix it. It happened because my security system had expired.I ended up paying with my Visa charge card. --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: Over65
396	98658795	8/7/2018	Waunakee, WI	Consumer got a pop on her computer that her financial documents were being jeopardize and to call Microsoft. Consumer called the number on the pop up and they stated that they will fix her problem for $545.73 which she did by providing a card number.
397	101853385	8/8/2018	Livonia, MI	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted] It will help if you provide the Microsoft reference number 63E1CFF9-8DC1-4730-AB82-AF82AD334A67. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- I was browsing my computer then a pop up shows up in my computer --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: Over65
398	98775252	8/10/2018	Cincinnati, OH	Consumer states that she receive a call from their tech support servicer, NTS IT Care Inc. stating they were going out of business and offered her a refund of $350. Consumer granted the caller remote access to the consumer and had her log into her bank account and was asked to enter refund amount of $200 but by mistake there was a refund of $20,000. Consumer was instructed to withdraw $20,000 out her bank account and send it back to them via FedEx. Consumer was then told they did not receive the money and was asked to withdraw $19,000 and send via UPS. Consumer later found out that it was their own money from her CC account, checking account and
399	101848339	8/12/2018	San Angelo	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted] It will help if you provide the Microsoft reference number A2FE2983-AC44-42AA-AAC6-057C2F6D3E4C. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- My computer was locked up and would not even shut off - instructions on page said to call for assistance resolving the malware (said Zeus) paralyzing my computer --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow
400	99059057	8/16/2018	Ocala, FL	See Attached Complaint

401	99035880	8/18/2018	Rhome, TX	In Jan, when my husband signed on to his computer he was blocked by a sign stating something to the effect that he must call that number, claiming to be MIcrosoft, becasue of a serious virus. I turned of his computer then back on and it worked fine but the next mornig the same message was there so hesitantly we called the number and did as they said. After all was said and done we had paid them $699.00 via credit card. They assured us the computer was safe and they would not call again. however on 8/17/18 they did call claiming that updates they had tried to install did not work so they must again access the computer. (I might add here that we frequently get calls saying something is wrong with our computer but we hang up on them). Anyway as you info states they are very convincing and i am totally ignorant on computers. (Just what they are looking for). Anyway ashamedly, i did give them assess to my computer and after about an hour they called back to say they found all sorts of stuff and showed me what was supposed to be proof but meant nothing to me. this time they promised to refund the original payment as their programs had failed and wanted me to go immediately to a store and purchase google play cards to the tune of $500 to $600. i then informed them that i must think about it because i had begun to believe it was a scam but then the real pressure to do as they asked began. when i refused to act Dave, who he claimed to be, said he would call back. in the meantime i called my son in law to confirm what i believed and he advised that it definately was a scam. I was still talking to him when Dave called back and my husband ta ked to him telling him we wanted nothing to do with him and his company. he argued and again stated his "reason" etc. Finally my husband told him that we had checked with our son in law who was in the frauds division. There was suddenly a dial tone in his ear. i also got an email from them giving a new number but this morning that email is gone. Other-Other Update
402	101851019	8/18/2018	Buena, WA	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 942FB498-3A56-4685-9E3D-B548A3963498. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- The person did get rid of the apparent virus but it took a long time and eventually had to speak to 3 different people. Was told not to contact MSFT but I am suspicious. Thecaller gave me a toll free number 1-844-2082608 for their comuter helpline. I was told they will call me again on Monday. I gave them a VISA charge card number for their charge of $651.59. Are they legitimate? --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: false --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: Over65
403	99116626	8/21/2018	San Ysidro, CA	On 8/16/18 in the morning, i was working on my home computer when an orange screen appeared with a loud warning message. My computer had been hacked! I was instructed to NOT turn off my computer, but to call the 877 number. Like a fool, I called and spoke to Jaime Mathen, who sounded East Indian or Pakistani, but he said he was a tech with NTS and that my computer had been infected. He brought up a screen that allowed him to take control of my computer. He then showed me a list of files that said were viruses. I did not recognize these files as any that I had made. He was able to circle in red what files were bad. He told me the good news was that this hack had only happened the day before so we caught it early. He asked me about other devices I had,(my deceased husban'd computer and an iPad) and he told me to turn those devices off while he worked on mine. I turned them off. He had me type certain keys, but he never asked for any passwords or user names. After deleting all the bad files he told me the charge for that was about $129.00, but that I really needed to purchase the NTS service, which I ended up doing for 3 years! That, plus the service fee, came to $894.30, which I charged to a credit card. I have filed a complaint with the credit card company, as well, for this charge. Jaime gave me one more telephone number, his personal number in case I ever had a futher "problem" with any device. The number is 1-844-208-2608 EXT 302. He also wanted to access my other computer, but I told him I couldn't turn it on and I would do so the following day. I did not turn it on and it is still off.What should I do now? Call my bank and the Credit Reporting Bureaus and change all my usernames and passwords? I feel like such a damn fool to have fallen for this, but my husband was the computer technician in the family and without him I am lost.
404	99250365	8/24/2018	Hyattsville, MD	Consumer states she called a phone number appeared on his computer to individuals claiming to be Microsoft stating they needed to gain access to her computer to fix the problem with her network.
405	101850932	8/24/2018	Washington	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 8E940090-36BA-46DD-A81A-8248B6688249. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- Pop ad blocked my computer. Had to call above number. James M. remotely access my computer. Said my computer was sending viruses over the internet. He was a MTS tec. for Microsoft Com. and had to remove the problems. He removed a few programs and requested my credit card $199 - $399 for virus removal. I refused. Computer blocked. I turned off. I contacted FTC with Scam report & MICROSOFT. --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: 50-65

406	99393377	8/29/2018	Winston Salem, NC	I was looking up information on our local school system WSFC. A pop up came on screen telling me the computer had a virus and it needed to be fixed immediately or the computer would be shut down and could not be restarted. My daughter nor son-in-law were not home, do I was willing to go through the process to get it fixed. They kept me on the phone so I could not call my family to apprise them of the situation. When they said they would call me back when the computer was fixed. I immediately called my daughter. She told me to shut it down. I did. I received two more calls from the number: I did not answer. My son-in-law came home. They called again and I gave the phone to him and he told them that they were scammers and he was not dealing with then.
407	100014115	8/31/2018	Benton, KS	Called me. Scared me into sending $700.00. Declared unfixable. Send $2000 more for new one . I balked. Local expert nothing wrong. A scam on elders I had received an unsolicited emergency alert several years ago warning me to immediately call NTS. I live in the country, dirt road, local service sporadic and very slow that day. I called. For several hundred they 'fixed ' the problem. On the 15th of May 2018, NTS called my cell phone directly. They had been 'monitoring ' my computer and declared I had a virus. Not sure how, still a mystery. After making my screen image shake a bit, declared a Trojan had attacked me. Need to send $700.00 by Google play cards immediately! They frightened me enough to drive 30 miles into town to buy a $500 and two $100 cards. They told me to scratch the back of the cards and read them the numbers. I had never bought one of these cards before but was reassured by the NTS representative that as long as I kept the cards in my possession that they could not get any money from the cards. Not true as I have found! However after sending the codes from the cards they then declared I needed a whole ' new computer '. I needed to dash back into town and send $2000 more. A Robert Hooper was to appear on my dirt road in the country in the morning with a new identical virus free computer, install it, take my old Sick Computer away and refund me my $700. Only by buying a new computer from NTS was I ever to get my $700 refunded. By this time I was getting suspicious and tired from rushing off 30 miles to buy Google Play cards. I am almost 80 and my wife asked me what I was doing. Upon hearing the details 'she put her foot down as well as my phone.' Too late Cards were cashed. I have pictures of a Refund Receipt from NTS as well as the Promises and ' Findings ' by Jordan and Jack White. The phone numbers given me on my computer bt ' Jack and Jordan ' ring but don't answer. A few days later my computer was checked by a local expert. No evidence of any viruses. Only thing sick was me at being scammed. Since then I have had two more unsolicited calls from 'NTS '. They somehow are still watching my computer and think I need more help. They know my cell number but deny that they took my $700. Lost forever they say. 'Write it off '. Different group they say, pretending to be NTS. Of course I have in my possession the computer message I printed from NTS stating they got my Google Play cards for $700. They did nothing but scare me and endanger my life frantically driving to town. --- Additional Comments: Send me $700 and never call me again
408	99491413	8/31/2018	Mechanicsburg, PA	Consumer is calling stating that she has received a pop up on her computer from someone stating to be from NTS IT Care. Consumer states that they told her that her computer is emitting a virus. Consumer states that they wanted remote access to her computer. Consumer did not provide access.
409	99517312	9/2/2018	Greenwood, IN	I was finishing reinstall for windows 10. Got everything up and running and went internet to download Norton by Infinity when a Microsoft error filled my screen I tried alt. ctl. delete but it would not take it off. So iI called the number to see what was going on with it. I fell into their trap. Shut them down they are playing dity pool! Other-Other Update
410	100952702	9/3/2018	Greenwood	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 625A11E0-61EE-4D20-81F3-DD89EFC49399. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- I was Scam by company who was attached to a microsoft fake web site domain --- Method of Contact: Other --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue
411	99538554	9/4/2018	Muskegon, MI	Consumer states that she received a phone call from NTS IT Care Inc.. Consumer states that she was told that a refund would be sent to her for but they wanted access to her computer again. Consumer later found out this was a scam
412	100953329	9/5/2018	Greenwood	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number D675D785-D857-4C2E-920E-BD526616A2BC. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- They pop up on MY COMPUTER SCREEN while trying to download NORTON security from Xfinity > Could not get them by using task manager. So I called their and fell for their trap. Please shut these guys down! --- Method of Contact: Other --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: Over65

413	99744415	9/10/2018	Columbus, OH	I was on my computer trying to go to my bank website and my computer froze with a message, sup pos ably from Microsoft, with overlay message saying not to turn off your computer and to call their number because my computer has been infected by a virus and or a multiple of other things. I called the number, they told me they needed to excess my computer to see how and what had infected it. Then they told me I'd been infected by a Trojan virus and it could of infected all computers in the house and my web root anti-virus would not stop it. In order to stop it, their company has a 3yr. Service that would protect everything from being hacked into. I felt vulnerable and needed to stop identity theft. After I bought into it they ran a scan and fixed the problem. Afterwards I looked them up and saw they have a lot of complaints filed with the BBB. Hopefully you can stop their scam. I have called my bank and I'm filing a complaint with BBB. I hope you can help me. Thanks! [redacted] Other-Other Update
414	99751398	9/11/2018	Mansfield, OH	Consumer said that a screen came up on her computer and she could not get it off and requested that she call a designated number and she did. The consumer was told they could unlock her computer for service fee of $199.99. The consumer then canceled her debit card.
415	100948943	9/13/2018	Greensburg, PA	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 74FD579C-8C08-4598-A0F0-7CCFBB3269A6. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- was told my subscription (that was on my Toshiba when I purchased it) had expired 7-2018. said had sent notification of expiration. Because it expired had to be renewed. said I had zeus malware that was infecting computer. pop up froze computer and referred me to this company at direction of Microsoft. Said all techs were Microsoft certified and were contractors for Microsoft. --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: Over65
416	100951840	9/14/2018	La Conner, WA	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 3E3D79F3-92F2-4DF8-BB7A-95F4C482B9E6. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- While working in MapQuest I encountered a controlled popup with a verbal message Your computer is infected with a virus. Call the number below immediately (888-658-0533) your computer wil be blocked from further use. Do not turn the computer off. Call immediately. --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue --- Consumer Age Range: 50-65
417	100960773	9/15/2018	Saint James, NY	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] a [redacted]. It will help if you provide the Microsoft reference number 02C699D0-D691-4035-9AEB-2ACEE9E21122. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- I received a blaring message and I could not access anything on my computer. It claimed that I was hacked and I had to call this number. They claim that they are an official IT company of Microsoft. I panicked as my brothers identity was stolen a few years ago. I gave them access to my computer.....They advised me that it was a server issue. I am sick to my stomach to think they havemy info --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue --- Consumer Age Range: 50-65
418	99917731	9/16/2018	Washington, MI	When I turned on my laptop it locked up and showed that i had a Porn Virus and to call this number to help me unlock it. I had suspiciions but I could not unlock my computer so I called them, They were all Indian but spoke very good English. They were very professional and I thought that they were legit. They accessed my computer and got it working for a 1 year fee of $199. They said they were located in California I think that there should be some way the FTC could notify everyone about these scam companies and what to do when their computers are locked up to get them going again without contacting these crooks. Other-Other Update
419	100956861	9/17/2018	Florence	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 72BDCFFC-895E-47CB-B4BB-2B0EF73DEE99. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: Other --- Other Software Name: not sure --- Consumer Age Range: Over65

420	100142540	9/21/2018	Belpre, OH	This company called me from a phone number 309-791-4140 saying they were NTS. They said I had malware and Trojan and my computer was going to crash. He said there were 9 different things going on. In order for him to fix it, I needed to buy four $50 Google play cards in order to get it fixed. I told him I only had $100. I bought two $50 cards and gave him the key card information. He said he would call me back on my pay day to get two more $50 Google play cards. I then gave them control of my computer in order for them to "fix". They then locked up my computer and I could not get in. My son had to disconnect my computer and buy me a new one.
421	101826436	10/2/2018	Corvallis, OR	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 67E8BC12-4508-424B-8C64-2A721EFDAB08. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- they ask for address phone # card # said not to install any other virus software. to call the number they installed on my computer. once they took my payment they told me that office was in Pakistan. --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: Over65
422	101504476	10/3/2018	Memphis, TN	These company called NTS IT CARE, I was on my computer about 2 weeks ago. And I had a pop up saying that you have a virus on your computer along with a number to call and they will clean my computer for 75 dollars. So someone told me that they were a scammers, so they were calling for payment which I didn't do. So I goes to turn my computer on and they have shut it off we're I can't cut it on. What do I need to do! --- Additional Comments: DesiredSettlementID: RepairCut my computer back on!!!!
423	100643838	10/7/2018	Des Plaines, IL	WHILE OSING MY COMPUTER ON FACEBOOK ON TUESDAY 10/2/2018, I CLICKED A LINK TO GER MORE INFO FROM AN ADVERTISER. I GOT POPUP SCREEN SATING MY COMPUTER WAS IN DANGER AND I NUST CALL THE DISPLAYED NUMBER FOR ASSISTANCE. COMPUTER WOULD DO NOTHING ES=LSE. SO I CALLED. VIK ANSWERED AND SAID I HAD A VIRUS AND HE COULD FIX IT, I ASKED IF HE WAS MICROSOFT AND HE SAID NTS CERTIFIED BY MS.SO I DID WHAT HE SAID AND IN MOMENTS HE WAS ON MY SYSTEM. FOUND THE ISSUE HE SAID AND DELETED IT. NO MENTION OF PRICE AR ALL. THEN PROCEEDED TO SELL ME 2 YR SERVICE FOR $300.00. GAVE HIM MY CREDIT CARD. NEXT MORNING SEARCHED NET AND FOUND NTS SCAMMERS. I CALLED AND CANCEL SERVICE AND THE BILLING AT NTS SAID COUL ONLY CREDIT 4170. as service mon was 130.. said ok only to try and get some back. they sent note thursday want me to acknowledge there$130. fee I did but still waiting. Transaction still pending at my credit card company.
424	100816958	10/8/2018	Des Plaines, IL	NTS IMPLIED THEY DID TECH SERVICE FOR MICROSOFT.THEY USED MY BROWSER TO DISPLAY MSG MY COMPUTER WAS HACKED AND TO CALL THEIR NUMBER TO RESOLVE.$300. $10/2/2018 MY COMPUTER DISPLAYED WINDOW WITH MSG MY COMPUTER HACK. CANNOT DO ANYTHING. CALL DISPLAYED NUMBER FOR SERVICE.I DID AND REP VIK SAID MY MACHINE WAS HACKED AND NEEDED TO BE REPAIRED.I LET VIK SIGN ON . 5 MIN HE HAD FIXED AS I BELIEVE IT WAS NOT HACKED BUT NTS HAD USED FACEBOOK TO PUT THEIR PROBLREM ON MY MACHINE. THEN HE SOLD ME 4300. SERVICE AGREEMENT FOR 2 YEARS.CHECKING THE INTERNET TODAY 19/03 I FIND THEY DO THIS ALOT TO GENERATE BUSINESS. I CALLED TO CANCEL AND GET REFUND. --- Additional Comments: FULL REFUND OF MY %300. NTS BILLING SAY THEY WANT $130.00 FOR PROBLEM THEY FIXED. i WANT FULL $300.REFUND AS THEY NEVER MENTION ANY FEE FOR REPAIRING 10/02 PROBLEM.

425	101613114	10/8/2018	San Diego, CA	Receipt of email stating that I have a contract that will expire and automatically renew. I have no records of this contract.Copy of email that I received Friday, Oct 5, 2018.COMPUTER REFUND <computerrefund100@gmail.com> [redacted] NTS IT CARE Priority:Normal Date:Friday, October 5, 2018 3:33 AM Size:8 Khi this email is from NTS IT CARE and the reason why we are sendingThis email to you because we like to inform you that the service which you haveSigned up NTS IT CARE with has been expired so the service will beAutomatically renewed today and the renewal charges will be $599.99 USDFor 3 years contract and it will be automatically debited from yourbank account becauseYou have signed a contract with NTS IT CARE for the auto renewal contractHowever if you don't want to continue with our service you can call onthis number +1304 933 9573This is our cancellation department number and ask NTS IT CARE tocancel the service andYou need to be in front of your computer to cancel the subscription.And we will like to inform you that the service which you have signedup for the computerProtection i hope you remember that you called us when you wore facingproblem withYour computer and quicken so we fixed the problem and you paid us certain amountand the invoice of that contract was sent to your email so kindly callus on +1304 933 9573if you wish to cancel the contract otherwise the contract will berenewed automaticallyand the money will be debited from your account and once it is debitedfrom your bank account youWill not be able to get any refund so if you wish to cancel it thencall as soon as you receive this email.office timing;10AM TO 4PMPlease avoid this email if you wish to continue our service.Thank youU.S.A+1 304 933 9573MANGER:ADAM SMITH --- Additional Comments: Proof of contract stated in their email.
426	100681325	10/8/2018	New York, NY	When I opened Amazon web site,pop up icon showed up and said that my Apple computer was infected by virus and took me to NTS IT care web site. I called company and spoke with James who said I have to pay $199 to fix my computer immediatly so I paid it. After that he got in my computer using remote access. Later, my wife called Apple support service and asked above issue then she was told that it was scam. My wife called NTs and spoke with Ammed who said they are innocent. He doesn't know why the pop up sign took their site. We still has to pay one time support fee which is $79 and I paid for it. I don't know he is saying a truth or not.
427	100662503	10/8/2018	Southport, NC	On or about 7/19/2018, a popup appeared on my computer screen telling me I had a virus. It gave me a number to call to have the problem corrected. I called the number and the tech support guy remotely took over my computer and supposedly loaded software which was supposed to correct the problem. I paid $419.00 by credit card for the software. Now I am getting calls from the company telling me they are no longer allowed to do business in the US, so they can't provide the software, so they would like to refund my money. They further state that the only way they can refund the money is by remotely connecting to my computer again. I refused to let them connect, and requested they refund the payment to my credit card. I reported this suspicious activity to my bank.
428	101827380	10/10/2018	Houston, TX	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted] It will help if you provide the Microsoft reference number 6421EF6B-3706-4266-BCAA-605B4B23A60D. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: true --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue --- Consumer Age Range: 26-49
429	100846286	10/12/2018	Rockland, MA	My husband was on the computer checking emails when an alert came on stating that it would not stop until this number was called. He called and they showed him several pages of default viruses, They stated that they would fix it for this amount. It would not shut off until he agreed even though he questioned that we had Noron anti virus. He paid $159.00

430	100847024	10/13/2018	Sunnyvale, CA	A pop-up apeared on my computer with a woman's voice saying my computer had been infected with a virus and I was to call the number 1-844-298-2608 right away. i called and a technician (Richard) told me how to get rid of the pop-up. He proceeded to tell me he could get rid of the virus and took over my computer. he further explained all the adware and mallware I had downloaded and my virus protection, Kaspersky, was an excellent program. He was with me on the phone for a good hourand that for $199.99 I could get tech support 24/7 for a year and also higher priced for 2 or 3 years. i told him I would take the one year and proceded to fill out all the information for my bank debit card. He then gave me to another tech who filled out an agreement giving them authorization to use the debit card to pay for the 199.99 charge. He then used an automatic signature of my name on the agreement. he also printed out a cooy on my printer for mr. He said they would contact me Monday to see if everything was OK. This all happened on a Friday. I am going to the bank this morning (Saturday) to see what has to be done. Other-Other Update
431	101959297	10/16/2018	Aliso Viejo, CA	This company sent a message on my mother's computer saying she has virus. She fell for the scam and they charged her $500.NTS IT care represented themselves as agents of Apple. They sent a warning spam on my mother's computer and she fell for the scam. They then told her they needed to clean her hard drive, installed anti spam software, fixed safari and installed Google. The charged her $500 for a 3 year plan. My mother is a senior citizen with Alzheimer's and was taken advantage of. When I called to cancel they were very defensive and said someone from billing would call us back. --- Additional Comments: Full refund on the business, assurance they did not take her personal information and ideally put this company out of business.
432	101281955	10/25/2018	Burlington, WI	Consumer received a call from someone posing to be Microsoft. He was told that he could help him fix his issue with remote access. Consumer was told that his bank account would get $2000. He needed to get a Google Play cards and give the card numbers. Consumer got a call form the bank regarding money transferred from his saving to his checking.
433	101824164	10/28/2018	Shreveport, LA	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigato [redacted] at [redacted]. It will help if you provide the Microsoft reference number 10B4C391-3164-4BF9-8E3B-55B923EFD285. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- THEY TOLD ME MY COMPUTER WAS INFECTED I WAS HAVING TROUBLE WITH IT. I WAS STUPID AND GAVE THEM MY CREDIT CARD AND PASSWORD TO MY COMPUTER SO THEY COULD FIX IT. WILL THEY TAKE MY IDENTIY WHAT SHOULD I DO. --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: IDontKnow --- Consumer Age Range: Over65
434	106069075	10/30/2018	TX	Tech Scam. reply pop-up --- AARP Type of Complaint: Scam/Financial Exploitation
435	103033673	11/6/2018	Rancho Santa Margarita, CA	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 8E92ACEE-3279-40BD-867A-D376DDABC8E1. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- wanted to help me with the Virus --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: false --- Consumer Age Range: 50-65
436	101700141	11/7/2018	-	Consumer reports that she got a pop up from someone claiming to be with Microsoft. She called the company call NTS IT Care who sold her their services for $200. She gave them access to her computer. She provided her Master Card number to pay for the services.
437	54798949	11/13/2018	New York, NY	Consumer called to report that she received two calls telling her that they were with Dell and her computer has viruses. Consumer paid 350.00 to have the viruses remove. Consumer called Dell and was this was a scam UPDATE 04/22/2015 Consumer is calling to provide additional information. Reports she continues to receive the calls, this time they pose to be from Windows [redacted] 09/06/18 UPDATE: The consumer received an email from a company that claimed to be Microsoft, and they told her they are going to shut down her ability to use Word, etc. [redacted] Update 11/13/2018: Consumer is calling to report that she is still receiving phone calls. [redacted]
438	101989192	11/16/2018	Shreveport, LA	The consumer states the screen on his computer lit up saying he was hacked and the computer was taken over. Consumer called a number on the screen for NTS Software Support and was told they had a contract with Microsoft to fix issues. Consumer was shown issues in his computer. Consumer was asked to pay 129 dollars but did not pay.

439	106224576	11/19/2018	Derby, NY	Note: The Consumer Sentinel Network cannot presently categorize this data contributor's Product Service Code. The comments field may have a description of the good or service offered to the consumer. --- NTS IMPLIED THEY DID TECH SERVICE FOR MICROSOFT.THEY USED MY BROWSER TO DISPLAY MSG MY COMPUTER WAS HACKED AND TO CALL THEIR NUMBER TO RESOLVE. $289 8/18 MY COMPUTER DISPLAYED WINDOW WITH MSG THAT MY COMPUTER WAS HACKED. CANNOT DO ANYTHING. CALL DISPLAYED NUMBER FOR SERVICE.I DID AND REP VIK SAID MY MACHINE WAS HACKED AND NEEDED TO BE REPAIRED.I LET VIK SIGN ON . 5 MIN HE HAD FIXED AS I BELIEVE IT WAS NOT HACKED BUT NTS THEN HE SOLD ME 4300. SERVICE AGREEMENT FOR 2 YEARS. They called back 11/9/18 saying they were unable to provide proper service and would l ke to give me a refund. They signed onto my computer and were in control of it, I told them I didn't want them to do anything but they continued. When I insisted they not do anything they said ok - then cursed and hung up on me. My computer was blank. I called my bank and the credit card company, the one used to pay initially, and they put alerts on accounts. I had to bring my computer to be fixed as I was unable to use it. That cost and additional $100 --- Consumer's Requested Relief: A refund of the $289 initially paid for "security service"and $100 needed to restore computer to useful state. --- Consumer County or State: ERIE --- Other Payment Method: DEBIT
440	102774550	11/19/2018	Dandridge, TN	They hacked my computer to pretend it had a virus and then proceeded to convince me to pay them $150 to correct. This appears to be a scam.They hacked my computer on 11/14 and presented a signal on my screen that suggested i had a virus and asked i call them pronto. The conversation suggested they were operating on behalf of Microsoft and offered to correct. The indication was that there would be no charge. They took control of my computer and after the work they gave me the option of 1-3 trs protection. I chose the 1yr @$149.99. I have had 2 calls since but refused to talk. At my request the bank has canceled my card as of 11/15/18 and are sending me a new one. I want my money back and would like to see this operation subjected to a criminal investigation before others are hurt. --- Additional Comments: Refund of $149.99 and investigation of the operation which appears to be shady and illegal.
441	102068529	11/19/2018	Rockmart, GA	Consumer states she went online and clicked on a website. She got a pop up and the number came up to call back. The tech Shawn Depay said he worked with Microsoft called Network Technology Services. She gave him access to her computer. She agreed to pay by 12/01/2018. When she called Microsoft she said they didn't work with NTS.
442	103035292	11/21/2018	Battlement Mesa, CO	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number B30EAE94-D5D0-4371-BF05-830D6A3C9C66. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- They remotely access my computer showed me what virus I may have and then asked for money to fix it --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue --- Consumer Age Range: 26-49
443	102178583	11/23/2018	-	MY COMPUTER STATED WITH LOUD FEMALE VOICE AND FLASHING LIGHTS STATING DO NOT SHUT DOWN, SOMEONE IS TRYING TO ACCESS YOUR COMPUTER, ETC. COULDN'T SHUT DOWN, AND THERE WAS A PHONE NUMBER LISTED. I HAVE A COMPANY THAT DOES MY SECURITY ALREADY AND I WAS LED TO BELIEVE THIS WAS MY COMPANY AND AFTER LOOKING INTO MY COMPUTER THEY FOUND A TROJEN VIRUS AND IT WAS GOING TO COST $399.99 TO FIX FOR THREE YEARS SECURITY. MY TRUE SECURITY COMPANY CALLED TODAY AND STATED THEY FOUND PROBLEMS AND FOUND THE BEGINNING OF RANSOM WARE DOWNLOAD. IT IS FIXED NOW, CALLED MY CREDIT CARD COMPANY AND CLOSED DOWN MY CARD AND HAVING GOLDEN ONE DEAL WITH THE $399.99. I CANT BELIEVE THEY DO THIS.TOPIC:Referrals
444	102178560	11/23/2018	Palm Harbor, FL	Consumer states that she received a pop up on her computer that looked like it was from windows and asked her to call a number. Consumer called this number and was told that she must pay to receive the services. Consumer hung up on the individuals. Consumer states that they claimed to be with Windows.
445	102390566	12/1/2018	Elizabeth City, NC	This is a follow-up to my earlier complaint today: reference # 102390177. I now believe, as does my family, that NTS IT Care is part of the scam. I got involved with them when trying to buy something on Amazon.com & was told that Amazon could not except my order because of viruses in my computer. They reportedly cleaned my computer and installed Norton Antivirus. How did the scammer in my original complaint (# 102390177) know to tell me that they had to take off the work orginiallly ordered and return my money without being all a part of the same scam. Both times a man named Ryan was involved and both had simialar accents.

446	102390177	12/1/2018	Elizabeth City, NC	A man named Ryan pretended to represent the company that services my computer NTS IT Care. In the above form I gave you the info regarding NTS BUT THE SCAMMERS PHONE NUMBER IS 623-562-1723. Ryan said he has to remove what he had put on my computer (Norton security etc.) and refund my $600 or my computer would crash. In checking my bank balance on line Ryan screen shot my acct and made it look like he had added a balance of $6000. I needed to give him back $5000 in Wal-Mart gift cards & giving him the gift card #s and pin #s (which of course he probably cashed immediately). Once home from the store I called NTS who said it was a scam and I shut down my computer & router. I have also closedd my bank acct. Ryan called again since he was booted off my computer. He had locked my computer & refused to unlock if if I didn't cooperate. The scammer called me 7 times the next day. The sheriff's deputy was @ my house filing a report) and spoke to the scammer. The scammer actually wanted to talk to the deputy! The scammer has not called back since.
447	102400416	12/2/2018	Cincinnati, OH	I am 81 years old and try to stay in contact with family on facebbook. I made the mistake of clicking on a news article and instead was a pop-up saying mycomputer had a virus and to call their number at NTS IT Care inc.I was afraid and was told that I needed antivirus for 249.00 I used a Visa and was told they would fix the problem. I later found out that this was part of a fraudulent scam that was actually listed many times on Google. I have applied for a new Visa card. I actually have avg antivirus so I know the pop-up could have been deleted if I knew how and I should not have called the number. I also gave them permission to control my computer from wherever they were working. Other-Other Update
448	103650850	12/3/2018	Germantown, TX	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number AFF65904-2A29-4B78-A734-31D3DDF1DBE3. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- They wanted me to pay $130.00 a year for the service of protecting my computer --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: false --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeInOrLogMeInRescue --- Consumer Age Range: Over65
449	102649149	12/9/2018	-	While on the computer, a popup screen came on and locked my computer- said my computer had a virus. In a different area, I saw the number for a virus protection company. I called the number (1-844-208-2608) and they said they could install a program to remove the virus and threat, and secure my computer. The cost for thier service was $299.99 for three years of protection. I paid this on my credit card and later found out this was a scam- this company was responsible for the popup. Other-Other Update
450	102827935	12/14/2018	Sharon, CT	The company accessed my bank account and attempted to remove $30000.00. My bank stopped the scam. I don't know what else they have.
451	103365494	12/19/2018	Muskego, WI	Entered in Complaint Wizard. See paper complaint for description details. --- Consumer Initial Contact: Other --- Nature of Complaint: Phishing/Spoofing
452	103041680	12/21/2018	Coatesville, PA	i was working on my laptop when i got a flashing screen from microsoft with a loud voice stating that i should not shut down or turn off my computer or it would be damaged. i did try to clear the screens, but it did not stop it. relunctally, i called the number on the screen and a man with an indian accent answered and said he would fix it. he found that my security was not on and there many bad files that he would remove. then he said that i could get 24/7 support for any issues i may have if i paid $300 for three years. since i was afraid that my computer was in danger, i agreed. now i have read complaints about these scams and would like to see if i can get my money back. thank you and God bless!

453	103148369	12/28/2018	Richardson, TX	10/26/2018: NTS IT Care put a virus on my PC, showing a warning about it being infected, files corrupted, and the only way to get out the frozen screen was to call them. I called and they got on my computer. They said the corruption was due to malicious ads, and they would clean up the files, install an ad-blocker program, and provide service for one year, for $199.99. I paid this amount by credit card and they sent me a receipt. They installed the AOL Shield Pro and Adblock Plus programs. 12/19/2018: William Marshal and Jordan Belfort from NTS called on 501-478-4422, and said that the software they had installed got corrupted and should be removed from my PC. They offered me to refund the $200. I let them to get on my PC to do the uninstall. I saw that they installed a TeamViewer program, so more people could work on my computer. For the "refund" they said the money must be sent on the same day, from their Chase Bank account. They showed their Chase Bank account in a window on the screen, and asked me to log in to my bank, so they could transfer the money. I did this and they insisted I fill out the Chase money transfer form. In their Chase form they had boxes for name, address and amount, but not for account number. When I tried to type in the $200.00 into the box, several additional zeroes were coming up. After three attempts I typed in the correct amount but saw in my bank account window that there was a new wire transfer deposit of $2,000.00 on my checking account. The entry did not show that the transfer came from Chase Bank, and only the next day did I realize that they transferred the $2,000.00 from my own money market account. They tried to tell me that I was at fault, for typing in the bigger number, and I denied this but could not prove that they did it. They insisted I return their overpayment right away. They said the only way to reimburse them today was to buy a $1,000.00 and an $800.00 gift card at the Apple store, and tell them the letter and number combinations on the back of the cards. I told them I was sick, and would do this the following day. They started to threaten me, saying I would lose all the data on my computer. I told them this was blackmail. I drove to the sore, bought the gift cards, and told them the card combinations. Later they told us that the "clean-up work" was not finished yet, and I need to call them the next morning, and in no case should I turn on the computer.12/20/2018: They called and said the same: clean-up not done, do not turn computer on. I tried to turn on the computer but they changed my password. On my laptop I checked our bank account and found out their illegal transfer of my own funds. I tried to call them but they did not pick up the phone. We closed our bank account, and opened a new one. I unplugged the PC and took to Fry's for repair and salvage of picture and document files. All the programs have been lost. The hard drive was damaged and had to be replaced. This was a $250 repair, not counting all the lost programs.My wife called Apple and explained the fraud and extortion scheme the criminals used to get the gift cards. The Apple case number is: 100711143842. I called Citicards, to contest the $1,800 charge to our DoubleCash Mastercard we used to buy the gift cards. 12/21, 2018: Jordan Belfort left threatening messages, saying I would be "in very big problem" and that he would sue me, if I did not call him back.
454	103640801	1/10/2019	Houston, TX	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number CFD859AE-A9FD-4850-923B-9E4F2E0A255C. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- I Was glad he help stop the noise. But I thought it was free then the toke my information then I see a price of $499.99. I told him I thought it was free. The he ask if I was a senior citizen. I asked why he asking personal questions . --- Method of Contact: I received a pop-up message on my computer --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: false --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: I dont know --- Consumer Age Range: 50 - 65
455	103639308	1/14/2019	Orlando, FL	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number B9D4EB42-0EC6-4DA0-9014-B732A901B24C. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- I got a pop up message that said to call Microsoft at once as my computer was hacked. Said not to try and exit page and to call Microsoft. Rep who answered gave me over to this company. Charged me $200.00 to fix problem. Just trying to find out if this is a legit co before I cancel payment and report to police. They are trying to contact me again. --- Method of Contact: I received a pop-up message on my computer --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeIn --- Consumer Age Range: Over 65
456	104791663	1/15/2019	NJ	Rcv'd call re: computer virus & charged $350 for tech support. --- AARP Type of Complaint: Scam/Financial Exploitation

457	103641724	1/18/2019	Portland, OR	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] a [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number C59240D0-BF43-4D8B-8B5A-581C5188B69F. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- Not sure if NTSITCare is actually fraudulent or if the dude who answered the phone was just directing me to their website to make him look legit. Did want to login to my computer but I wouldnt let him.It started with a re-direct from IE that took over IE. Claimed computer was super infected etc. Wouldnt let me close it out or anything. Finally used Task Manager to kill the task. Then call --- Method of Contact: I received a pop-up message on my computer --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: false --- Consumer Age Range: 26 - 49
458	103553319	2/4/2019	Deposit, NY	Consumer states he received a phone call from individuals claiming to be Network Technology Services stating they could help him secure his computer, individuals asked for $50 dollars via debit card, consumer did comply.
459	104092887	2/18/2019	Marietta, GA	MY WIFE WAS ON THE COMPUTER WHEN A LOUD NOISE OF BELLS AND HORN SOUNDED WITH A VOICE SAYING YOUR COMPUTER HAS BEEN LOCKED AND HAS A VIRUS WITH A DISPLAY TO CALL A PHONE NUMBER. SOUNDS WOULD NOT STOP TILL I CALLED NUMBER DISPLAYED A PERSON NAMED JACK ANSWERED I EXPLAINED WHAT HAPPENNED HE SAID I PROBABLY HAVE A VIRUS AND OFFERED TO CHECK IT IF HE COULD TAKE CONTROL OF MY COMPUTER. I AGREED TO HAVE HIM CHECK IT. HE TOOK CONTROL AND POINTED OUT A WEBSITE THAT CAUSED THE PROBLEM. HE THEN OFFERED TO CORRECT THE PROBLEM FOR A FEE OF $499.99 WHICH I AGREED TO AND PAID BY CREDIT CARD KNOWING IF THIS WAS A SCAM I COULD DISPUTE THE FEE. HE INDICATED IT WOULD TAKE 30 MINUTES TO COMPLETE AND WOULD CALL ME BACK.HE CALLED BACK AND SAID TASK WAS COMPLETED. COMPUTER SEEMED TO BE OPERATING OK AND ENDED CALL. I CHECKED THIS COMPANY ON THEIR COMPANY WEBSITE AND THE BETTER BUSSINESS WEBSITE FINDING IT HAD A NUMBER OF COMPLAINTS SIMILAR TO MY EXPERIENCE WITH OTHERS OVER THE PAST FIVE YEARS.I FEEL THIS COMPANY MANIPULATED ME AND DEFRAUDED ME 0F THE AMOUNT I PAYED. I CONTACED THE CREDIT CARD COMPANY CITI AND DISPUTED THE CHARGES AND CLOSED MY ACCOUNT IMMEDIATELY AND THE SUGGESTED TO CANCEAL CARD AND WILL SEND ME NEW CARDS. I FEEL I HAVE BEEN VIOLATED AND THIS COMPANY NTS IT CARE NEEDS TO BE INVESTIGATED. THANK YOU AND IF I CAN ASSIST YOU FURTHER PLEASE CONTACY ME.
460	105253353	2/19/2019	Stow, OH	Computer was held hostage until a 'fee' was paid, once the fee was paid my computer was released back to me.On January 17, 2019 my computer was frozen, an alarm was going off and was asked to contact this company to fix my computer. I called them and was told that I had to pay $499 so my computer would work again. I didn't know at the time that is a scam. They released my computer and was able to continue. --- Additional Comments: I am looking for the full refund of the transaction which is $499.99.
461	104691959	2/19/2019	Virginia Beach, VA	see attachment --- Additional Comments: see attachment
462	104407399	2/20/2019	Macon, MO	A pop up appeared on my computer and they told me I had a virus, I paid $399.00 with my credit card to remove it. I later learned this was a scam and was able to stop the transaction with the help of my credit card company. IsVictim:false --- Initial Means of Contact: Unknown
463	104190955	2/20/2019	Avon Park, FL	The consumer reports a message on his screen stating to check file system. Consumer states he had been contacted by this company 3 years ago and was offered protection for a fee. consumer did agree and later discovered it was fraudulent.
464	105691184	2/23/2019	Las Vegas,	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] a [redacted]. It will help if you provide the Microsoft reference number 0F579F0B-2DC7-4B47-888B-E4AC6695BAA6. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- Wanted me to call back when I get the money to pay for the service. --- Method of Contact: I received a pop-up message on my computer --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: I dont know --- Consumer Age Range: Over 65

465	104161077	2/25/2019	Cranbury, NJ	I got on my laptop loud noice . and it says to call that number for firewall to clear my computer . i call the number 1855 338 3777 then thety shared my computer . i allowed them because they said they were apple. they let me agree on lots of pages i dont know what it is. asked for $299 i gave them my credit card . but i got mess on my cell to aprove i did agree. then later when continuing with them i said no do not charge since they are not affiliated with apple . they cancel the charges.but what they made me sign i dont know what else they can get. they asked if I am senior and if i do on line banking I said yes but did not give them bank info. I cacelled my credit card i gave them .and i changed my PW for on line banking. i am afraid if they can get any credit card in my name or my husband name. since this happened after me trying to get to my husband email which I am allowed it did failed couple to times , then this what happened. if they got to share my computer with me. what else can be happend. Please help also another tel they have 1844 659 9899 thank you. UPDTE: 2/25/19 Consumer inquired if there was an update on her complaint. [redacted]
466	105691203	2/26/2019	Tempe, AZ	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 8D9B81D9-E23B-4BC7-9092-D68426345715. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- Received pop up message on my computer that my computer was blocked and not to shut it off but to call microsoft phone # 1/833/337-7751.A woman named Arem Johnson logged into my computer and told me my drivers and system was very corrupted and that their tech support [Ronny] would fix the problem for $300 [Dennis]. I will cancel the charge once its posted to my acct. Will make police report --- Method of Contact: I received a pop-up message on my computer --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeIn --- Consumer Age Range: Over 65
467	104472394	2/28/2019	West Covina, CA	I was doing an internet search and clicked on a website which caused a lot of pop-ups and loud spoken warnings to occur, saying that my computer had been infected and that I should not turn off my computer. The warnings, which appeared to be from Microsoft, said that I should call 1-844-659-9899 and they would step me through how to repair my computer. I stupidly called the number and allowed the guy (Peter) to take control of my computer. He proceeded to show me how my computer was infected and did a great job selling me a protection package and also said they would clean out the viruses. I paid by credit card after being transferred to their billing office. Since then, however, I have had my computer repaired at a local tech shop, removing every trace of that company, though that has been an additional expense. I called my credit card company and because I have fraud protection on the card, they dropped the charge and changed my card number. NTS IT Care is very slick. Please put them out of business! 1605 S Main St #125Milpitas, CA 95035-6270http://www.ntsitcare.com/
468	104621510	3/4/2019	San Diego, CA	NTS IT Care used a malicious browser pop-up to disable my computer. This malicious pop-up falsely claimed my computer had a virus and to call them. I called NTS IT Care and they remotely accessed my computer, then asked me to pay them $300. When I stated I needed to think about it, NTS IT Care employee Richard Jones threatened me, stating my information would be compromised and I would lose access to my account. At that point I became supsicious, ending the call and powering off my computer.
469	104787098	3/8/2019	Boyertown, PA	I was interrupted while working on my desktop computer by a message telling me to call a phone number or else my computer would crash in a few minutes. I couldn't figure out how to stop the message, so I called the number and was told that several viruses were infecting my computer, and that NTS IT CARE would fix the problem if I paid them $299. I gave them my Citi Card number and the last four digits of my SS. NTS IT CARE took control of my computer and said that they fixed the problems. The computer seems to be working ok. Last night on NBC news I heard that a scam was going around. I became suspicious. So I did some research on the internet and discovered that some web sites warned that NTS IT CARE is a scam outfit. Can you tell me if this is true. If NTS IT CARE is not a legitimate company, can I get my money back? Thanks for your help.
470	105694565	3/11/2019	Raleigh, NC	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number BBABA96D-9D52-4BFB-BA0D-CE1F41CBCA5B. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- When I called the number stated from the pop up on my computer (pop up stated there was an issue with microsoft edge the representative gave his name as Lee Thompson with employee ID NTS IT-012. He stated that in order for him to repair my computer he would have to access my computer. I let him do so he used log me in. I begin asking more questions and asked if this was free? --- Method of Contact: I received a pop-up message on my computer --- Fraudulent Person Claim to be Microsoft: Yes --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeIn --- Consumer Age Range: 50 - 65

471	104997590	3/13/2019	Redding, CA	Working from home pop-up web page locked my computer and gave me their number for Microsoft support. Stated my computer was infected and would be damaged if I didn't call the number for service. After calling was told they could fix the problem for one of their pricing options and my computer would not be usable without their service. Agreed under duress and let them have remote access to my computer and after charging my card they did something to fix the problem. I later canceled my card and disputed the charge. Most importantly as a work from home medical transcriptionist I lost a full day of work since after they "fixed" my computer I left it turned off until I could determine if they had installed any malicious software.
472	107132352	3/14/2019	Redding, CA	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted]. It will help if you provide the Microsoft reference number 37EEEF9D-71D2-423C-89E4-8FB2872A21A0. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- Pop-up locked my computer and said to contact Microsoft support tech at 855-528-4222. My wife not realizing it was a scam contacted them and was told she needed to pay them and give them access to fix her computer or it would be unusable. Insisted on payment which included a one two or three year service policy. I later cancelled the card numbers they were given and have filed FTC complaint. --- Method of Contact: I received a pop-up message on my computer --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: true --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeIn --- Consumer Age Range: Over 65
473	106533058	3/19/2019	Whitesboro, NY	Received a pop up on computer locking me out and claimingI had a virus. Claimed I needed a One Time Fix on MAC computer.11/14/2018, (Purchase Date), Party ID: 700aaae7-9e55-4e66-9d94-e5db482df34bCC'd Recipient Ip: 172.17.210.663 yr. Service Plan - $349.99; Paid by VISAI had given up on settling this problem, but have noticed all the recent complaints towards this company. I am a 78 yr. widow who received a pop up on my MAC computer locking me out and claiming that I had a virus, to call a certain phone number, etc. Very high tech tactics to convince me I had to purchase this extended software support warranty to resolve the 'virus??' I am not computer savvy!! My daughter tried to call the company back for me after I realized this was not legitimate and had to end up yelling at the sales rep. stating I did not want this 'Plan' with no response. I had contacted my Credit Card Company and my Attorney to no avail. I could not prove the SCAM!!!! Very upsetting to be taken advantage of!! --- Additional Comments: I would definitely seek a total refund as I do not need this service or intend to use it at all!! I am not a person to be on the computer for even 1hr. a week.
474	105757078	3/28/2019	Puyallup, WA	They tell you that you don't have things on your computer like Virus Protection then they sell it to you and take away the virus protection you did have. First they lock up your computer and find that after you turn it on. They took a lot of money from me and I want it back. IsVictim:true --- Initial Means of Contact: Unknown
475	107129247	3/29/2019	Tillamook, OR	Note: At this point, Microsoft does not provide specific consumer fields. For that information, please contact Technical Support Fraud Paralegal [redacted] at [redacted] or Senior Investigator [redacted] at [redacted] It will help if you provide the Microsoft reference number C387E982-96C4-4CCD-B602-86E0365E421B. If that does not work, please contact customersupport@consumersentinel.gov. Please note that due to length, the Microsoft reference numbers appear in the Complaint Disposition fields. Complaint Narrative: --- A FULL SCREEN POP UP CAME ON WITH MICROSOFT LOGOS AND AUDIO SAYING DO NOT SHUT DOWN COMPUTER AND THERE WAS ONE OF SEVERAL THINGS WRONG WITH MY COMPUTER. I CALLED NUMBER ON SCREEN TALKED TO A NATHAN FOR ABOUT 20 MINUTES AND ALLOWED REMOTE ACCESS BEFORE I REALIZED HE WAS A SCAMMER AND HUNG UP ON HIM BEFORE GIVING CC NUMBER. --- Method of Contact: I received a pop-up message on my computer --- Fraudulent Person Claim to be Microsoft: No --- Fraudulent Person Claim to be Microsoft Partner: true --- Fraudulent Person Use Hostile Language: false --- Fraudulent Person Access Computer Remotely: true --- Remote Access Software Name: LogMeIn --- Consumer Age Range: 50 - 65
476	105715019	4/2/2019	Houston, TX	This "NTS ITCare" company said that a hacker had gotten access to my computer and that I needed to provide Google Play cards to them becasue they acted as security. I bought $9,200 of these google play cards, and they received the codes. They told me that they woul be delivering me a check to reimberse me for these Google Play cards as well as bring me a new laptop and computer as hackers had information to the computer I am currently on. This morning, 4/2/19, they said they had a check for 15,300 for me and that since i only paid 9,200 in the google play cards I needed to go and buy the remaining 6,100 worth before they could bring me a check and the computers. They had remote access to my desktop computer and told me to not shut it off. I shut it off last night before I went to sleep and they are saying I was not supposed to do that since they are protecting my information on their end. This morning they asked me to log on to my banks to verify that the hackers did not mess with my bank accounts. They told me how to turn off the remote acces (so that they could not see my bank information) but there was still a yellow line around the screen. They said I could only check my bank through the desktop and not through mobile banking since the hackers were located on the desktop. The people I have talked to are Steve Wa ker, who was the tech support, and the technician who was supposed to bring me the check and computers, Robert Hooper . They also got me in contact with "Google" in which I spoke to Austin Williams who claimed to be a Google Supervisor and when I asked for a "@google.com" email he hung up the phone. I have kept all of the receipts and play cards that I gave them.

477	105843233	4/4/2019	Magnolia, DE	On Feb.22nd 2019, while I was typing on my computer, the screen went blank and then shrill alarm signals followed with the screen blinking off and on "Warning!!! Your security has been compromised!!!! and for me to call a number connecting me to Norton Security Systems.As my computer was not responding to anything after that, I called the number and the individual said he would call me back immediately. He did and advised me that they had been notified that my security had been breached and if I wanted to purchase the Norton Security Package (he gave me prices for 1,2 and 3 yrs., I opted for 3 years at the price of $ 389.98 which I paid with my debit card. After that he requested that I give access to my computer so they could fix the glitches and remove the cookies and whatever else supposedly compromised my computer. The whole process took approx. 2 hours. The amount was withdrawn from my account on Feb. 26, 2019 by NTS IT CARE INC 877-490-6709 CA. On Apr. 2nd I received a call from the same individual identifying himself as Steven Anderson and as the man who had previously contacted me. He asked if my computer was okay to which I answered that it slowed down considerably and his answer was, that that was the reason for his call. They had supposedly received a lot of comlainnt calls and deducted that the program they installed was faulty and therefore they were issuing refunds to all plus an additional $ 100 for the trouble caused. I asked how that was supposed to happen to which he replied that I would have to again give their tech access to my computer so I could fill out a refund form and my bank information so that could transfer the funds. I would get $ 150.00 up front and the remaining $ 350.00 in a couple of days. I had to fill out a form with the amount scheduled for transfer and when I typed $ 150.00 and clicked the enter button an amount of $ 15000 appeared at which point he freaked out because that number could not be changed and I would now receive that amount in my account. If his company would find out he would get fired. He asked me to check my account to assure me that the money was in there and of course as his Tech was still on my computer working "the glitches" they then also had access to my account and showed me a deposit of $ 15.000. But the screen was not exactly the same as my usual screen on my online banking. He made me close it and reopen it to make sure that I thought the amount was in there. He wanted me to return this amount minus the $ 150 = $ 14.500 to which I replied I would gladly do so as soon as the money is in my account I would return it to where it had come from (he had mentioned Chase Bank earlier when I questioned him) but now he said I couldn't return it there because they would find out and he would still get fired. He gave me a Bank, account number and account holder in Panama. I told him I would not feel comfortable sending money there and would go to my bank to assure that the money was actually in there, which of course it wasn't. He stayed in contact with me when I was at the bank but refused to speak with the bank manager at which point I refused to pay anything unless it showed up correctly. He tried to give me another bank info, this time from Suntrust in Florida, advised that a transfer had been made - which it had, but it was an in-house transfer from my savings acct to my debit acct before we had a chance to change passwords. Then I said I would report this. I did not do transfer