STATEMENT OF
ROBERT BURDA
INTERIM CEO/CHIEF STRATEGY OFFICER
CYBERCRIME SUPPORT NETWORK

BEFORE THE
COMMITTEE ON OVERSIGHT & REFORM
SUBCOMMITTEE ON NATIONAL SECURITY
JULY 13, 2022

Chairman Lynch, Ranking Member Grothman and members of the subcommittee, thank you for inviting me to speak with you about the state of cybercrime and the impact it has on our military and veteran community. My name is Robert Burda and I serve as the Interim CEO and Chief Strategy Officer for Cybercrime Support Network (CSN). Our mission is to serve individuals and small businesses impacted by cybercrime. We accomplish this mission via:

- FightCybercrime.org: an extensive website of resources to help cybercrime victims recognize, report and recover from over 45 different types of cybercrime.
- Our Peer Support Program: A 10-week virtual support group for romance scam survivors.
- Our Military & Veteran Program: A program that enables us to deliver cyber safety training and education directly to active duty service members, veterans and their families at no cost to them. This program will be the focus of my testimony today.

The military and veteran community is made up of active duty, reservists, guardsmen, veterans and their families, totaling more than 22 million Americans.[1] Throughout their service and beyond, these individuals encounter transitions which make them more vulnerable to cybercriminals who take advantage of these transitions and the unique aspects of military life to carry out fraud, stealing hundreds of millions of dollars from the military and veteran community each year.

Cybercrime's Growing Impact on the Military and Veteran Community

Cybercrime continues to have a growing impact on the military and veteran community. Reports to the Federal Trade Commission (FTC) from the military and veteran community as a whole have nearly doubled from 125,000 reports submitted in 2018 to 206,000 reports submitted in 2021.[2] In addition, financial fraud losses reported by military consumers have tripled from $81 million to $266 million between 2018 and 2021.[2]

Veterans account for approximately 18 million of the over 22 million Americans that make up the military and veteran community,[3] which could explain why their losses are highest among this community. From 2018 to 2021, veterans and military retirees accounted for the highest number of reports to the FTC, with more than 441,000 reports submitted and $345 million in financial losses reported.[2] Service members — including active duty, reserve and national guard — submitted over 83,000 reports totalling more than $99 million in financial losses, and military

spouses and dependents submitted almost 85,000 reports totalling more than $72 million in losses.[2]

The FTC is one of only a few sources of data that underlines cybercrime's devastating effects on the military and veteran community. Their work is both needed and greatly appreciated. However, this only gives us a small glimpse of the overall impact cybercrime has on our men and women in uniform. Generally, cybercrimes go unreported because victims either don't realize they have been victimized or don't think what has happened is a crime. The FBI estimates that only 15 percent of American fraud victims report these crimes to law enforcement.[4] Until we significantly increase the likelihood of someone reporting a cybercrime, it is unlikely that we will know the full scope of the problem.

Aspects of Military Life Spark Opportunities for Cybercriminals

Being a part of the military and veteran community comes with frequent transitions—including deployment, relocations, discharge and retirement—which open windows of opportunity for cybercriminals. During deployment, service members are away from friends and family with limited contact, often leaving their spouse solely responsible for household financial decisions. Many military families find themselves with orders to move from one state or country to another every few years. When it's time for retirement or discharge, service members must rapidly assimilate back into civilian life often after many years in the military community.

Throughout these transitions, service members, veterans and their spouses are frequently requesting and sharing documents and personal information to access benefits exclusive to this community—such as buying a home with a VA loan, using GI Bill benefits for themselves or dependents, or managing other veteran benefits. This creates a unique opportunity for cybercriminals to pose as representatives from government and military agencies — such as the Department of Veterans Affairs —using fake websites, spoofed phone numbers or forged email addresses in an effort to steal personally identifiable information (PII) from members of the military and veteran community. In fact, imposter scams accounted for the most money lost by the military community in 2021, with $103.9 million in financial losses reported to the FTC.[2]

In addition to imposter scams, Cybercriminals target members of the military and veteran community for a multitude of other online scams and fraud. Online shopping scams accounted for the second highest dollar amount lost by military consumers in 2021, with $29.6 million in losses reported to the FTC.[2] Financial losses due to job opportunity scams — typically directed at recently retired service members transitioning into civilian life — totalled $12.9 million in 2021.[2]

Lastly, cybercriminals take advantage of the military community's prominent use of social media. Surveys show that military members use social media more than civilians across the board.[5] This technology provides an easy avenue for this community to stay connected with their friends and family, as well as each other. Even military recruiters are using social media to reach

younger generations—one Army recruiter gets nearly half of her recruits from TikTok.[7] However, from the perspective of a cybercriminal, social media functions as a simple way for them to find information about their targets. Cybercriminals are able to obtain sensitive information from social media — such as how long someone is deployed, birthdays, locations, phone numbers and names of family members — and can easily create fake profiles as bait to implement these scams.

CSN's Military and Veteran Program

CSN's Military and Veteran Program is an alliance of over 40 organizations, corporations, foundations and federal agencies — including the Department of Veteran Affairs, Disabled American Veterans (DAV), Comcast, AT&T and Deloitte — to promote safe data care practices in the military and veteran community via webinars, online education materials and social media posts. In support of this program, a Public Service Announcement[8] was aired by Comcast over 33,000 times in 10 military-centric markets, including Ft. Myers, FL and Colorado Springs, CO. In addition, our partnership with VA has provided us the opportunity to air the PSA in 85 VA medical centers and 30 community-based outpatient clinics with more than 108,000 veteran patients visiting these facilities daily.

As we enter the next phase of our Military and Veteran Program, we are working to collaborate with military installations, veteran service organizations and military service organizations that will enable us to deliver cyber safety training and education directly to active duty service members, veterans and their families at no cost to them. We see a need for direct service and training throughout each aspect of military life and believe we are well-positioned to meet that need.

Recommendations

CSN recommends that the federal government directs financial support towards organizations, like Cybercrime Support Network, to deliver comprehensive online safety training to the military and veteran community at each stage of their transition. In addition, we strongly encourage your support of The Cyberspace Solarium Commission's proposal for a federally supported National Cybercrime Victim Assistance and Recovery Center[9] to serve as a nationwide cybercrime reporting and recovery program to support not only the military and veteran community, but civilians and small businesses too.

---

[1] Department of Defense: 2020 Demographics Profile of the Military Community. 2020. [Accessed: Jul 7 2022]. Available from URL: https://download.militaryonesource.mil/12038/MOS/Reports/2020-demographics-report.pdf.

[2] Federal Trade Commission: 2021 Consumer Sentinel Network Data Book. 2021. [Accessed: Jul 7 2022]. Available from: https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports.

[3] U.S. Census Bureau: Those Who Served: America's Veterans From World War II to the War on Terror American Community Survey Report. 2020. [Accessed: Jul 7 2022]. Available from: https://www.census.gov/content/dam/Census/library/publications/2020/demo/acs-43.pdf.

[4] IC3: Virtual Complaint Desk for Online Fraud. Federal Bureau of Investigation. 2017. [Accessed: Jul 7 2022]. Available from: https://www.fbi.gov/news/stories/ic3-virtual-complaint-desk-for-online-fraud.

[5] Statista: Refuel Agency Military Explorer 2020 Survey. 2020. [Accessed: Jul 7 2022]. Available from URL: https://www.statista.com/statistics/1130021/hours-spent-social-media-us-active-duty-military-members/.

[6] Alwine R. 6 Ways Military Spouse Facebook Groups Are Actually Helpful. Military.com. 2020. [Accessed: Jul 7 2022]. Available from URL: https://www.military.com/spousebuzz/2020/02/11/6-ways-military-spouse-facebook-groups-are-actually-helpful.html.

[7] Howe, E. Army Recruiters on TikTok Dance Around Ban To Reach Gen Z. Defense One. 2021. [Accessed: Jul 7 2022]. Available from URL: https://www.defenseone.com/policy/2021/11/army-recruiters-tiktok-dance-around-ban-reach-gen-z/186881/.

[8] Cybercrime Support Network. "Military and Veteran Program, Comcast PSA." YouTube video. Oct 6 2021. Available from URL: https://www.youtube.com/watch?v=V9xZoicX3FE.

[9] Cyberspace Solarium Commission: National Cybercrime Victim Assistance and Recovery Center Act. 2021. [Accessed on: Jul 7 2022]. Available from URL: https://cybersolarium.org/wp-content/uploads/2022/05/Recommendation_PAN1.3b.pdf.

Digitally signed by Robert Burda
Date: 2022.07.09 19:07:04 -04'00'