FCC NEWS from the Federal Communications Commission

FCC Media Contact:
MediaRelations@fcc.gov

DHS Media Contact:
mediainquiry@hq.dhs.gov

For Immediate Release

FCC WARNS TELECOM COMPANIES OF OBLIGATIONS TO PROTECT ACCESS TO CONSUMERS' CELL PHONE ACCOUNTS AND SENSITIVE INFORMATION FOLLOWING DEPARTMENT OF HOMELAND SECURITY'S CYBER SAFETY REVIEW BOARD REPORT

Enforcement Advisory Highlights Risks and Obligations Relating to SIM Swapping and Port-Out Scams

WASHINGTON, December 11, 2023—The FCC's Privacy and Data Protection Task Force today issued a new warning for mobile phone service providers regarding their obligations to protect consumers against cybercriminals who use scams that commandeer their customers' cell phone accounts.

The new warning is consistent with the findings released by the Department of Homeland Security (DHS)'s Cyber Safety Review Board (CSRB) in August, that outlined how threat actors from a global extortion-focused cyber hacker group engaged in fraudulent SIM swaps to carry out data breaches in furtherance of ransom and extortion schemes.

Today's Enforcement Advisory reminds telecommunications service providers of the increased threat of fraudulent SIM swapping, their obligations, and the FCC's enforcement priorities to protect consumer privacy and sensitive data.

This Enforcement Advisory incorporates provider requirements established by the FCC's newly adopted rules to help protect consumers from cybercriminals and scammers who target data and personal information by covertly swapping SIM cards to a new device or porting phone numbers to a new carrier without ever gaining physical control of a consumer's phone.

"Cell phone service providers are high-value targets for cybercriminals and scammers because in many instances they serve as the primary means consumers use today to access their most important and valuable financial and personal information. Bad actors are keenly aware of this and seek to exploit vulnerabilities to access this information. Telecom providers' responsibility to protect that data is vitally important," said Loyaan A. Egal, FCC Enforcement Bureau Chief and Chair of the Privacy and Data Protection Task Force. "The Enforcement Bureau will aggressively protect consumers' privacy and sensitive data and we will hold accountable carriers to ensure they are doing everything possible to combat these cell phone account access scams."

"We applaud today's enforcement advisory and the FCC's actions to protect consumers from SIM swapping," said DHS Under Secretary for Policy Robert Silvers, who serves as Chair of the CSRB. "The CSRB called for federal regulators to step up oversight of telecommunications providers to ensure they are taking all reasonable steps to prevent SIM swapping, which can cause devastating consequences to victims. Today, the FCC is doing just that."

The CSRB is an unprecedented public-private initiative that brings together government and industry leaders to deepen our understanding of significant cybersecurity events, including the root causes, mitigations, and responses, and to issue recommendations, based on this fact-finding in the wake of those events. Its second review, which prompted FCC action, examined the recent attacks associated with Lapsus$, a global extortion-focused hacker group. The CSRB found that Lapsus$ leveraged simple techniques to evade industry-standard security tools that are a lynchpin of many corporate cybersecurity programs and outlined 10 actionable recommendations for how government, companies, and civil society can better protect against Lapsus$ and similar groups.

The Bureau's Enforcement Advisory reminds telecommunications carriers of their duties and obligations to protect customer information generally, and specifically in order to combat fraudulent SIM swapping schemes that harm consumers and the broader public safety. A telecommunications carrier's failure to reasonably protect customer information, including through fraudulent SIM swap schemes, can independently violate the law. Such failures can result in fines or other actions by the Commission.

Carriers are further required to immediately notify customers of certain account changes including whenever a password, customer response to a carrier-designed back-up means of authentication, online account, or address of record is created or changed. These specific notification requirements are critical, but they are only part of the legal obligation to protect customers' information, which must take into consideration the nature of the vulnerabilities and what is known about threat actors.

To build on existing protections and to further combat the rising threat of these account scams, the FCC adopted new rules revising the FCC's Customer Proprietary Network Information (CPNI) and Local Number Portability rules to require wireless providers to adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or provider. Once effective, the rules will require wireless providers to immediately notify customers whenever a SIM change or port-out request is made on customers' accounts, and take additional steps to protect customers from SIM swap and port-out fraud.

###