DREHER TOMKIES LLP

ALERT

FOR CLIENTS AND FRIENDS OF DREHER TOMKIES LLP

April 21, 2015

FCC ISSUES ITS LARGEST PRIVACY AND DATA SECURITY ENFORCEMENT ORDER

The Federal Communications Commission recently entered into a Consent Decree with AT&T Services, Inc. for the purpose of terminating the FCC's investigation into whether AT&T violated 47 U.S.C. Sections 201(b) and 222 of the Communications Act of 1934 (the "Act") and corresponding rules at 47 C.F.R. Sections 64.2010(a) and 64.2011(b) in connection with data breaches at AT&T call centers in Mexico, Columbia and the Philippines. The settlement includes a $25M civil penalty, which the FCC says is its largest privacy and data security enforcement action to date.

The Consent Decree describes AT&T as a telecommunications carrier that provides mobile voice and data services to customers throughout the United States and the second largest wireless carrier in the United States, with over 100 million subscribers. According to the FCC's Order, the Consent Decree resolves its investigation of whether AT&T failed to properly protect the confidentiality of almost 280,000 customers' proprietary information, including sensitive personal information such as customers' names and at least the last four digits of their Social Security numbers, along with customer proprietary network information ("CPNI").

Section 222(c) of the Act is entitled "Confidentiality of Customer Proprietary Network Information" and provides that except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer CPNI by virtue of its provision of a telecommunications service may only use, disclose, or permit access to individually identifiable CPNI in its provision of (i) the telecommunications service from which such information is derived, or (ii) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

According to the Consent Decree, the FCC's rules require that carriers must (i) take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI and (ii) notify designated law enforcement authorities of a "breach" of its customers' CPNI as soon as practicable and in no event later than seven business days after reasonable determination of the breach. Section 64.2011(e) provides that a "breach" occurs when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. Section 64.2011(b) requires a carrier to provide notice of a breach to the United States Secret Service and the Federal Bureau of Investigation through an online portal.

AT&T informed the FCC that it discovered that three employees of an AT&T vendor that provided Spanish-language customer support from an inbound call center located in Mexico accessed customer accounts and obtained information, including names and the last four digits of customers' Social Security number, that could then be used to submit online requests for cellular handset unlock codes. AT&T maintained and operated the systems the Mexico call center used to access AT&T customer records and they were governed by AT&T's data security measures. According to the Consent Decree, those measures failed to prevent or timely detect a large and ongoing data breach. The personal information of some 51,000 customers was used to place 290,803 handset unlock requests. Additional data breaches involving approximately 211,000 customer accounts in AT&T's Colombian and Philippines facilities also were discovered.

The Consent Decree requires AT&T to, among other things, develop and implement a compliance plan that will include at a minimum (i) a risk assessment reasonably designed to identify internal risks of unauthorized access, use, or disclosure of personal information and CPNI, (ii) an information security program, (iii) ongoing monitoring and improvement, (iv) a formal internal compliance review, (v) development of a compliance manual and (vi) establishment and implementation of a compliance training program.

As the FCC stated in its press release regarding the Consent Decree, the FCC cannot, and will not, stand idly by when a carrier's lax data security practices expose the personal information of hundreds of thousands of Americans to identity theft and fraud. The FCC indicated that it will exercise its full authority against companies that fail to safeguard the personal information of their customers, international operations notwithstanding. ❑

✧ *Mike Tomkies and Margaret Stolar*

Darrell L. Dreher
ddreher@dltlaw.com

Elizabeth L. Anstaett
eanstaett@dltlaw.com

Margaret M. Stolar
mstolar@dltlaw.com

Robin R. De Leo
robin@dreher-la.com

Susan M. Manship
smanship@dltlaw.com

2750 HUNTINGTON CENTER
41 S. HIGH STREET
COLUMBUS, OHIO 43215
TELEPHONE: (614) 628-8000 FACSIMILE: (614) 628-1600
WWW.DLTLAW.COM

Michael C. Tomkies
mtomkies@dltlaw.com

Charles V. Gall
cgall@dltlaw.com

Judith M. Scheiderer
jscheiderer@dltlaw.com

Susan L. Ostrander
sostrander@dltlaw.com

Emily C. Barlage
ebarlage@dltlaw.com