April 9, 2015

As noted in previous **alerts**, the FCC has dramatically increased its enforcement of data security practices and breaches resulting from what the FCC considers to be inadequate security measures. Most recently, the FCC entered into a $25 million **settlement** with AT&T Services, Inc. (AT&T) resulting from the unauthorized access to personal customer information by employees of foreign-based call centers under contract with AT&T. The FCC again stressed that it expects telecommunications companies, which now includes broadband internet access providers, to take "every reasonable precaution" to protect their customers' data.

In this instance, call center employees based in Mexico, Columbia and the Philippines, used log in credentials to gain unauthorized access to customers' names and partial social security numbers. This information was then sold to third parties to be used to unlock AT&T mobile phones that had been stolen and sold on the secondary market. The systems used by the call centers were governed by AT&T's data security measures, which "failed to prevent or timely detect a large and ongoing" data breach. The FCC order does not provide information on the types of security measures AT&T utilized but notes that AT&T was implementing new monitoring procedures.

When obtaining the customer name and social security number information needed to unlock phones, these employees also accessed, but no evidence suggested that they used or disclosed, the specific type of customer information called customer proprietary network information (CPNI), which includes information such as telephone numbers called. In addition to agreeing to a $25 million payment (no information was provided on how this number was obtained), AT&T also agreed to a detailed compliance plan.

The FCC found that the employees' unauthorized access violated the statutory privacy provisions contained in Section 222 of the Communications Act, and also constituted an unjust and unreasonable practice under Section 201(b) of the Act. These two provisions will also be applied to providers of broadband Internet access service once the FCC's new Net Neutrality Order becomes effective.

Several interesting aspects of the FCC's self-described "Largest Data Security Enforcement Action" should be noted by entities subject to the FCC's jurisdiction. First, this breach involved company insiders with access to the company network. Media coverage of recent data breaches, however, has frequently focused on threats from the outside (e.g., from nation state actors and Advanced Persistent Threat (APT) actors). Awareness of insider threats has not been as prominent. This situation shows that such threats from employees cannot be ignored.

A variety of actions can be carried out by entities to address these insider threats, including but not limited to identity management, data classification, and implementation of access controls. Identity management involves both technology and processes that permit or deny an employee's access to certain assets, as appropriate. It can include such things as two-factor authentication and password management. Data classification allows data to be tagged and access to the data to be limited by use of access control technologies. The combination of these and other tools can be used to minimize the ability of people with authorized access to the network to engage in unauthorized access of information to which they do not have rights. Companies should also consider ongoing vetting of employees to make sure that they do not pose a threat after they have passed the initial background checks.

The FCC's action also helps quantify potential risk exposure. Just based on the $25 million settlement, the cost of the breach works out to approximately $89 per record that was unlawfully accessed. Although this is less than the commonly cited average data point of $200/record in commercial data breach situations, this settlement amount does not include the additional costs of customer notification, "clean up" of the breach, and the ongoing monitoring costs. The settlement amount does, however, provide an

estimate of the types of exposure companies might be facing based on the number of records they possess. (In a previous data breach **order**, the FCC indicated that it would apply a base fine of $29,000 per record based on existing agency forfeiture rules).

Ultimately, the FCC continues to focus its efforts on data security situations. It notes that it has "taken five major enforcement actions" in the past year. Of those, the first three were privacy related (involving robocalls, violations of do-not-text requests, and unlawful marketing). The latter two, including this one, both focus on cybersecurity. It appears that the path forward by the FCC is clear—cybersecurity is definitely in the agency's cross-hairs. Please contact our Telecommunication practice team and our Privacy & Data Protection team if you have any questions about this or any other cases.

Key Contacts

J.G. Harrington Washington, DC	jgharrington@cooley.com +1 202 776 2818
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090