Levine Blaszak Block & Boothby LLP

**Cash, Credit… or Cellphone?**
***Wireless devices are on the road to becoming the next credit card. Is your enterprise ready?***

**Andrew M. Brown**

Over the last 18 months, innovative applications for wireless devices have proliferated. In the enterprise space, the potential costs of that pose a serious challenge to any telecom group that has grown accustomed to predictable costs for wireless services. Indeed, the traditional "one-two punch" of competitively procuring wireless services and aggressively optimizing rate plans during the term of your wireless agreements, while still necessary, may no longer be sufficient when it comes to controlling wireless costs.

Now, corporate buyers need to stay ahead of—or, at least, keep pace with—their employees (often referred to as "corporate-liable users" or "CRUs") using new applications on wireless devices paid for by the company, especially when those applications may add unexpected charges to wireless bills. One such application, in wide use throughout the rest of the world but still in its infancy in the US, is the use of a cell phone to purchase goods and services. Through a variety of technologies and processes-- RFID swipes, texting key words to a specified address, or embedding credit card account numbers in SIM cards, to name three—wireless devices can substitute for credit cards, with purchases charges appearing on the device's monthly invoice.

If you haven't thought of your CRUs' wireless devices as credit card equivalents, change your thinking. Luckily, US wireless carriers, merchants, credit card companies, and payment processors have not yet reached agreement on the allocation of payments and fees necessary to allow widespread roll-out of "cellphones as credit cards." But it's just a matter of time before they work through these issues. The resolution of these competing interests in other parts of the world -- notably Asia where wireless devices are widely used to make purchases -- and the growing availability even in the US of wireless device payment for niche products such as parking meters, suggest that the use of wireless devices to make payments for all kinds of things in the US will soon be commonplace.

Even in the absence of widespread deployment, enterprises can still face unexpected charges on their CRUs. Within 10 days after the devastating earthquake in Haiti earlier this year, some $30 million had been donated to relief efforts by individuals texting $10 donations from their wireless devices. A number of enterprise customers subsequently learned that some of these donations had been made by their employees

using CRUs. Just like that, the donation had become a payment obligation of the company.

Having to address the issue after the fact created an uncomfortable dilemma: should companies attempt to rescind contributions that were made by their employees for largely benevolent reasons even if the contributions were not authorized? Rescinding the donations or seeking payment from the employees was, given the circumstances of the disaster and the nature of the contribution, awkward at best. Most companies swallowed hard and paid the bills.

But this situation, and the ones likely to occur in the future when wireless devices are widely usable as payment devices, can be avoided by taking a couple of common sense steps:

First, negotiate the issue with your wireless carrier before any undesirable charges are incurred by your employees. Carriers should be amenable to blocking services that apply text donation or other charges if they know up front that your organization does not want to authorize such charges.

Charitable contributions aside, think about whether your company wants to authorize charges for non-telecom goods and services for which the carrier is performing billing and collection for third parties. If that is something that your company is not interested in, make sure your contract specifies that you do not want to purchase such services and that you will not be liable for payment of such charges if the carrier fails to block them. As is always the case with unauthorized charges, if you do not have strong contract language that allocates to your vendor responsibility for blocking these charges, you will have to spend a lot of time and energy fighting them when they appear. And if your contract did not prohibit the charges in the first place, you will likely be on the hook for payment.

Second, if you don't want to address the issue (or already have a contract in place that does not address the issue), establish an internal policy for your employees that provides guidance on the permissibility of these charges and makes employees responsible for unauthorized charges to their CRUs.

For ages, large corporations have had policies governing the appropriate use of corporate credit cards by employees. But relatively few have adopted similar policies governing the use of wireless devices and the types of charges the company is willing to pay on behalf of the CRU subscriber. Adopting an internal "acceptable use policy" for CRUs can address a number of issues associated with employee use of company owned

wireless devices: prohibited activities, data security, employee obligations to report loss/theft, etc.

If your organization decides to permit wireless devices as a payment tool, your policy can outline permitted (and prohibited) charges, just like any other corporate reimbursement policy. But as we've learned with other use policies for mobile devices, a policy is only as strong as the mechanism you employ to enforce it. For this reason, we suggest backstopping employee use policies with technological tools, namely, blocking of certain services and applications, either though your own mobile device management platform, or through the carrier.

If, on the other hand, you want to prohibit such charges but do not want to involve your carrier in the decision, you can simply prohibit employees from incurring such charges and, if the charges appear on a wireless bill, allocate responsibility for their payment to the responsible employee.

Note that if you don't involve your carriers, you own the problem. Your ability to enforce a policy against employees will depend in the first instance on your ability to find the unauthorized charges. If you rely on a TEM provider to perform this function, you may have to put in some extra effort to make sure the charges are caught (which, depending on your TEM contract, may require payment of additional fees).

The charges are coming. If you want to keep control over your wireless bills, take the time now to think through and implement a few commonsense measures.

***Andrew M. Brown*** *is a partner in Levine, Blaszak, Block & Boothby, LLP ("LB3"), a Washington, DC based law firm dedicated to the representation of large enterprise customers, including nearly half of the Fortune 100, engaged in the procurement of network services and related technologies. Andrew can be reached at abrown@lb3law.com.*