



# Corporate vs. Employee-Liable Mobile Devices

April 2009



Every company that utilizes mobile devices as a business tool is often faced with this dilemma: purchase mobile devices under the corporate account (Corporate-Liable Units – “CLU”) or allow employees to purchase their own (Employee-Liable Units – “ELU”).

Mobile devices are fast becoming an essential business tool. To compete in the global economy, corporations utilize mobile assets to work more efficiently and stay in touch with their clients and colleagues. Managing these devices, however, is no easy task. To alleviate the management issues, some companies have decided to disperse the responsibility to their employees. These companies may have exhausted their resources and options and decided to convert to ELUs. Other companies may have grown too fast and have not the chance to rein in the mobile devices that their employees are using for business. Whatever the reason may be, there is a danger in using ELUs as company business tools.

Here are some key attributes corporations should consider when choosing between CLUs and ELUs:

- Ability to enforce security measures and policies
- Cost in terms of actual spending and management cost
- Visibility of usage and spends
- Protection of corporate data
- Negotiation power with carriers
- Grade of service from carriers

In this document, we will explore the pros and cons of each option.

### **Employee-Liable Unit (ELU)**

A corporation may choose ELUs over CLUs for various reasons. Management may be frustrated with managing their mobile devices. With employees coming and going, it is difficult to keep track of the devices and associate them with the end users. Employees have no visibility to their own usage, since invoices are sent to the company, not employees. If the employees’ names are not properly registered with the carriers, these employees cannot call the carriers directly for support. They have to turn to their company’s internal help desk instead. Yet, the internal help desk is created to address computer-related problems, so the support team may not have the expertise to handle mobile device-related issues. By choosing ELUs over CLUs, companies no longer have to deal with these issues.

Yet, choosing ELUs over CLUs can expose the company to many risks. Data devices can contain gigabytes of the company’s information. Some companies allow their employees to receive corporate e-mails on their personal phones. They may even allow employees to access their corporate files through their ELU devices.



This posts a major risk because companies cannot impose security measures on these ELUs. When the devices are lost or stolen, or when an employee leaves, the company has no authority over these devices to regain control of the data.

Another issue companies with ELUs face is that they cannot impose corporate policies on personal mobile devices. Companies cannot disallow employees from texting while driving. They cannot require employees to use hands-free devices when operating an automobile. They also cannot control the type of information these employees send or receive on these devices. Yet, the company may still be liable when employees misuse their devices while at work. For example, a company may be liable when an employee causes an accident sending an e-mail to a client while driving.

The cost of ELUs is actually higher than CLUs. Why? First, the minutes on these devices cannot be pooled, so a low-minute user cannot offset the high-minute user's usage. Secondly, employees who are reimbursed a set amount may be reluctant to utilize their devices fully when their limit is reached. The main purpose of a mobile device is to allow employees to stay connected with clients and colleagues. If employees are not utilizing these devices for fear of having to pay out-of-pocket fees, then it defeats the purpose of issuing the devices in the first place. Thirdly, employees have to spend time managing these devices. They are the ones on-hold with the carriers when they have issues. Because they are not treated as corporate clients, they may have to line up in carriers' stores. This can take away their productivity time. Also, if an employee has issues with a data device, the IT department cannot call the carrier directly to troubleshoot the device. The employee must call the carrier, along with the IT department, to resolve these types of issues.

There are other problems with ELUs that companies may not have predicted. To some employees, their mobile invoices may be the only expenses they have. They now have to spend time every month to submit their expense reports to accounts payable. Accounts payable also have to spend additional time each month to process these reports, then create and send the reimbursement checks to employees. Another hidden issue is that carriers run credit checks on each new device and require those with less-than-stellar credit to deposit a high fee before issuing the devices. Employees who face this problem may forego having a phone all together.

In summary, here are the pros and cons of ELUs:

Pros:

- No mobile management overhead to company
- Employees are responsible to pay invoices and handle carriers
- Fixed monthly costs (if reimbursed a set amount monthly)
- Employees carry one phone for business and personal use

Cons:

- No control over corporate data



- Lack of ability to enforce security measures
- Cannot impose corporate policies
- No uniformity in devices
- No visibility and control over employee usage
- Higher costs in actual spending
- Higher costs in lost of productivity
- Reimbursement may not cover actual usage cost (if reimbursed a set amount monthly)
- Employees' time to submit expense reports
- Increase in resources to process expense reimbursement
- Some employees lack credit to activate new phones

All company assets should be corporate-liable. Laptops and desktops are corporate-liable (unless an employee uses a home computer to access the company network. In this case, companies have ways to authenticate the users.) Even the staplers and pens are corporate-liable. Then why do companies allow their employees to own one of the most important assets within an organization? A mobile device can contain critical company information. It can contain corporate e-mails, files, and even customer contact information. With so much confidential information stored in these devices, shouldn't a corporation own them, not the employees?

### **Corporate-Liable Unit (CLU)**

CLUs allow for security enforcement, centralized management, and lower costs than ELUs. True, there is management costs involved. Companies need resources to manage these devices. Yet, mobile devices are now a requirement to compete in today's global economy. Companies should look at these management costs as part of their mobile program. When companies utilize the right tools to manage these assets, the total costs of owning CLUs can be much lower than owning ELUs, while keeping these important devices under control.

Let's look at the few downsides with CLUs. Aside from management issues, employees lack visibility into their own usage. Invoices are sent to the companies, not the employees. Employees do not see their own usage and spends. This issue can be easily resolved by implementing the right tools. Companies can provide individual reports to these employees to self-monitor usage and spends. Managers can receive "roll-up" reports to manage their own team's mobile devices. With the right tools, the telecom or IT department can disperse some of the management responsibilities down to the individual departments and users, while the time to review these reports can take less time than reviewing the carriers' invoices.



Employees may also complain that they have to utilize two devices, one for work and one for personal. To mitigate this, some companies have allowed their employees to utilize their business phones for personal purposes within reason. With the right tools in place to monitor total usage, personal usage will not dramatically increase the cost of issuing CLUs.

CLUs offer more benefits than ELUs. The main benefit is security control. Companies can enforce security measures, such as installing security software on devices, wiping data over-the-air, or simply terminating a device that is lost or stolen. Companies can require password-protection on these devices. They can also prevent users from installing applications on these devices. Mobile devices are becoming as powerful as computers, and the same measures imposed on computers should be imposed on mobile devices as well.

Another benefit is centralized management control. Again, with the right tools, companies can have complete visibility over their usage and expenditures. They also have better negotiation room with the carriers. Carriers provide better support plus special device and plan pricing to corporations. Depending on the size of the accounts, carriers also provide better procurement and invoicing tools. With CLUs, companies can choose the devices that work best for their requirements. Also, if a certain device needs upgraded software or is recalled, the company can conduct a mass-software upgrade or replace all the devices at the same time, saving employees the frustrations in resolving these issues on their own.

CLUs actually cost less than ELUs. Because companies can negotiate better discounts, they usually pay less in monthly plans and features. Companies can also utilize pooled or shared plans to balance low-usage users with high-usage ones. Pooled plans provide one of the biggest savings. In addition, with centralized management, employees are not wasting valuable time managing their own mobile devices. A side benefit is that carriers provide employees of business clients with special discounts for their own personal plans.

In summary, here are the pros and cons of CLUs:

Pros:

- Security control
- Centralized management
- Better business discounts and plans
- Business-grade supports from carriers
- Lower cost through pooled/shared plans
- Less management time required from employees
- No expense reports to submit and process

Cons:

- Management overhead
- Internal support to end users



- No visibility of usage and spends to end users
- End users need to carry two devices for personal and business

All the negatives of owning CLUs can be easily mitigated with the right mobile management tools. These tools may only add an additional few dollars per month per device. ELUs, in contrast, can cost two to five times more in hard and soft costs, in additions to creating security risks. CLUs are clearly the right choice for companies.

### Summary

This section compares the differences between CLUs and ELUs:

	CLUs (w/o mgmt tools)	CLUs (with mgmt tools)	ELUs
Centralized Management	✓	✓	✗
Visibility into Usage and Spends for Company	✓	✓	✗
Visibility into Usage and Spends to Employees	✗	✓	✓
Better Business Discounts	✓	✓	✗
Better Business Support	✓	✓	✗
Ability to Pool Minutes	✓	✓	✗
Security Control	✓	✓	✗
Resources Required for Invoice Processing	✗	✓	✗
Resources in Managing Carriers	✗	✓	✗
Lower Total Cost	✓	✓	✗