

Near Field Communications Holds Big Promise for Retailers, But New Headaches for the Contingency Planner



By [Leo Wrobel](#)

Date: Mar 15, 2011

[Return to the article](#)

Have you made a credit card purchase today? If you are like most of us, the answer is probably yes. But upcoming changes in technology might make whipping out the plastic as endangered as the handwritten check. Author Leo Wrobel explains how your phone may soon replace your credit card, and with that change will come a whole new area of concern for the contingency planner.

If there has been one thing about disaster recovery over the past 30 years, it is the fact that any new technology typically outpaces the means to recover that technology by three years or more. Years ago when mainframe computers were king, critical applications and financial data were safely locked up in a glass house computer room run by a professional MIS department. At that time, if one could back up the mainframe, the rest of the job was easy. Then along came Local Area Networks (LANs), and for the first time critical data was out there on desktops where it could be easily compromised. It is safe to say that a decade or more was spent trying to write new operating and security standards just to plug the vulnerability holes created by LANs.

Just about the time all that was accomplished, along came laptops, PDAs, and other handheld devices. The specter of a CEO dropping his or her PDA in a busy airport and the resultant consequences to the company (from stock manipulation to confidential email addresses being compromised) was the stuff that kept auditors up at night with cold sweats.

Now it's the wireless phone's turn. Moreover the problem may be personal this time. Rather than just affecting a corporation with a fiduciary responsibility to protect assets, a mishap with these new technologies may also affect you personally.

What Is Near Field Communication?

Manufacturers will soon be adding a new technology to the next generations of smartphones. The technology is called *Near Field Communications* (NFC), facilitated by a NFC chip in the phone, which will allow the person carrying a phone to make purchases in stores by simply swiping the phone over a reader. Sounds very convenient, doesn't it? It's a fact that most everyone carries his or her phone with them all the time, doesn't it? So what's the problem?

The first issue is that companies like Apple, AT&T, and Verizon will have direct access to the phone owner's confidential banking info. They would logically have to in order for this system to work. In this new paradigm, a person's phone would work the same way as a debit card, and would draw money from a bank account for the purchase. According to some sources, all this is coming along much sooner than we think.

The new Apple iPad is supposed to come out this spring, and NFC might well be one of its features. Make no mistake, the technology is coming. It's just too irresistible to equipment manufacturers like Apple and AT&T to roll it out.

First, consider that the technology will belong to companies like Apple, RIM, Nokia and by implication AT&T and Verizon. Banks and credit card companies need not (necessarily) apply. Apple could become the new middleman with transactions going through them instead of say, Chase or Citibank. Apple also might not have to pay processing fees to credit card companies, like it does now when people make iTunes purchases. And what about those pesky slow-paying wireless phone customers? Collection issues could be a breeze for AT&T and Verizon when payment

could be debited right out of the phone, right?

How Will It Affect How I Work?

How might this affect you at work, particularly if you are a contingency planner? First, many commercial organizations will have to purchase phone readers, assuming the technology catches on and that they want a piece of the pie. Consider the OPay Passo Exxon uses, where people wave their car keys in front of a pump before they tank up. NFC technology could extend this kind of convenience to virtually all purchases. While on one hand this can mean new business, it also means new operating and security standards for the retailer or company. What happens, for example, the first time someone hacks a phone to make a \$10,000 purchase at a jewelry store? Yet, by not accepting this payment method, the jeweler may be excluding a lucrative customer. Balancing revenue against risk is always the device's own dilemma. NFC technology may complicate this balancing act even more.

So what should contingency planners and corporate auditors consider when devising operating and security standards for these devices? Obviously if an employee's phone has NFC technology and they lose it, the wrong people may start charging things to a company account. Even worse for the employee, personal financial information may well be in the phone as well. That only makes sense because people need to split spending between accounts, in much the same way they use corporate or personal credit cards depending on the purchase. A tank of gas for the company car goes on a company card. Chuck E. Cheese for their son or daughter's birthday goes on a personal card. The burning question here should be in the event an NFC-enabled device is lost or stolen, will there be ways to freeze spending and avoid the financial hit?

A Phone Is a Credit Card, Too

People should always be careful with their phone, but arguably the urgency is here anymore. Ten years ago, the big fear was someone getting hold of one's phone and calling India for six hours. Nowadays this isn't the case. Long distance fraud has all but vanished because long distance has all but vanished. Even considering places (mostly overseas) where it has not, most people know wireless companies will readily write off fraud on a cell phone. It's just not an issue for them anymore. But when NFC technology comes into use, all bets are off. People are going to have to be educated that a phone is a *credit card*.

Consider that if I drop my credit card in a busy airport and it is used by the finder, my liability under federal law is a long-established \$50. Debit cards are a little different, but essentially it's a maximum \$50 liability if the issuing company is notified within 60 days. There are protections for online use of credit and debit card info both by the government and industry, and services like PayPal and Google provide peace of mind as well. What is the impact of all of this antecedent case law when one drops a cell phone? Frankly, I have no idea, and that's what concerns me should concern you too until rules and standards are codified.

What Should We Do Right Now?

First, learn to be careful with your personal or company phone in the same way you're careful with credit cards. In the event a device is lost, having the ability to shut it down remotely if it was lost would be great. Rumor has it that Apple phones will have this capability. Also, don't use your child's name or husband's birth date as a password. Make it tough for the finder to crack the phone and use it for illicit purposes. Of course this also depends on a standard that passwords will be used on these devices in the first place. While many of our phones have this capability, how many of us really use it?

Final Thoughts

Will credit cards become obsolete? I don't think so. I still write checks for some things, but it's becoming increasingly rare because one can use a debit card for most purchases these days. In one respect NFC will be just another mechanism for people to make purchases, but it's worth watching if you are a contingency planner or auditor. NFC promises to be convenient, and the wireless phone companies will see a lucrative new profit stream by cutting out the credit card companies and becoming the middle man themselves.

I keep one folded-up check in my wallet for the rare occasions I am in a place that does not take a credit or debit card. Perhaps people will keep one credit or debit card in their wallet after this technology comes along, in case their

cell phone battery dies, they are out of wi-fi or 4G range, or they drop and breakheir phone. After all, contingency planning scales down to the most basic level, does it not? Good luck in your plannig.
