

**Brigham Young University students will try out RFinity's microSD NFC card, installed in handsets, to purchase items at the school's bookstore and make encrypted peer-to-peer transactions.**

By Claire Swedberg

July 24, 2009—[Brigham Young University](#), located in Rexberg, Idaho, will begin piloting a mobile phone payment and security system this fall, provided by technology startup [RFinity](#). The system includes RFinity's microSD security cards, which employ Near Field Communication (NFC) RFID technology, and the pilot is intended to test whether the technology can provide secure financial transactions at the school's bookstore, as well as peer-to-peer transactions between students.

The technology was first developed in 2006 as a mobile phone security solution by RFinity's cofounders, CTO Steve McCown and CEO Aaron Turner, when, while working for the [U.S. Department of Energy](#), the duo were trying to develop a means of preventing data theft and unauthorized access to PCs and mobile phones. McCown developed a hardware security module for cell phones that included an NFC chip so that a phone could communicate with an RFID interrogator.



Aaron Turner, RFinity's  
CEO

The security module offered encryption to ensure data stored on a phone could not be accessed by unauthorized individuals, as well as an NFC tag that could transmit a unique ID number to an NFC reader, for use at secure locations such as a classified workplace in which cellular phones are typically prohibited. In the latter case, the phone could be tapped against an NFC reader on the door of a secured space, and the ID number would be verified as belonging to a phone approved for use in that space. In that way, the user would not have to surrender his or her phone while within that classified workplace.

In 2007, Turner and McCown began working together to leverage the module's security and NFC aspects for other purposes. They developed a highly secure NFC module to enable college students and other users to conduct financial transactions with contactless capabilities in their cell phones. The two attained a patent on the technology in 2008, built a prototype of the RFinity microSD security card, and received support from venture capital firm Horizons Ventures Ltd.

When using the mobile phone's battery power, the card creates a series of random, constantly changing encrypted ID numbers that link to a single, permanent, unique 16-digit ID number, initially generated and assigned to the user. Because these encrypted numbers are computationally impossible to predict, data thieves are unable to steal a user's unique ID number and use it to access that person's account. The security is built on the [National Security Agency](#) (NSA) Suite B standard—a strategy for protecting national security information—with elliptical curve cryptology (ECC) based on the algebraic structure of ellipses. "We never say our system is unhackable," Turner says, noting, "We do say that we are the

most secure contactless technology being developed today."

In September 2009, as the school year begins, RFinity plans to launch the first pilot at Brigham Young University, which is initially utilizing the system only in its bookstore. RFinity will provide approximately 100 students and faculty members with cell phones equipped with an RFinity security card, which is inserted into the microSD slot found on many mobile handsets. The school already provides each student and employee with an I-Card—a magnetic-stripe financial card that allows them to pay for goods and services on campus and have funds deducted from an account they establish on campus. In the pilot, the RFinity NFC payments will link directly to the I-Card payment system.

When a participant uses an I-Card to pay for items at the bookstore, he or she swipes the mag stripe on the back of the card at the point of sale, then provides the card itself to the cashier, in order to verify the picture. With the RFinity system, pilot participants could save as much as 30 seconds off their transactions by tapping the phone against an NFC reader at the point of sale.

As long as the payment is below a yet-to-be determined threshold (expected to be \$20 or \$30), the payment is automatically deducted from the user's I-Card account and the transaction is completed. If the payment cost is above the predetermined threshold, the participant punches in a password after tapping the mobile phone against the reader. The system can be configured to operate with the phone turned on or off, although a connection with the phone powered on offers greater security.

Between October and December of this year, RFinity intends to gain partnership from several local banks, allowing pilot participants with local bank accounts to use the phone as a debit card with money deducted from their bank account if they so choose, rather than from the I-Card account.

The next phase of the pilot will begin in January 2010, Turner says, when as many as 1,000 microSD cards will be made available to participants to install in their own cell phones. Initially, the card will be used with LG and some Motorola phones that support [Qualcomm's BREW](#) software platform, though by next year, RFinity expects the card will be able to operate with JAVA, Android, Windows Mobile and Blackberry platforms, as well.

The cards, which can act as both an NFC RFID tag and an NFC reader, will then be utilized not only at the bookstore, but also for person-to-person transactions, such as a private sale of an item from one student to another. If, for instance, a student wishes to sell his used textbook, he can simply choose from selections on the phone, indicating what he is selling, along with the price, then press "sell." The buyer can then tap his phone to the seller's phone and press the selection to purchase the item, and the seller can press a prompt to transmit the transaction information to the RFinity server, where the money can be deducted from the buyer's account and added to that of the seller. "For peer-to-peer transactions," McCown says, "our design requires the phone to be powered on."

By Dec. 31, Turner says he hopes "to have solid metrics from the first phase of the pilot," which he indicates will prove the security of transactions, as well as ease of use. At the end of the school year, he

adds, he anticipates being able "to prove the market opportunity for peer-to-peer use." The company is planning a North American product launch for summer 2010, and a subsequent launch in Europe and Asia, though the exact dates for these implementations have yet to be determined.

"Our system provides the high-security platform that third-party partners could build on top of," Turner states. RFinity is already in discussion with some of those types of partners, such as entertainment companies that could enable the purchase of concert or movie tickets on mobile phones. The phones could then store that ticket information and enable the user access to the paid-for movie or concert, by tapping the phone against a reader at the site of the event. It could also be used by hotels, he says, whereby a customer could pay for a room by tapping his mobile phone at a terminal at the front desk, then utilize the same phone to open the room door.

According to market research firm [Strategy Analytics](#), approximately 60 percent of cellular phones manufactured this year have a microSD slot. "The purpose of the microSD card is to provide NFC to phones without the technology," McCown explains. "However, we can also use our microSD security chip to augment NFC-capable phones," such as the Nokia 6131. "In the case of integrating an RFinity security microSD card with phones such as the Nokia 6131, the benefit is that the transactions would enjoy the protection of our encryption technologies."

While the iPhone does not have a microSD slot, McCown says, RFinity has met with [Apple](#), which has given his company a framework "within which we can craft a solution at some point in the future."