Imagine you are standing on the bus, when someone’s briefcase bumps into you, near your back pocket. “Sorry,” the man says. As you get off the bus, you notice the man got off at the same stop. As you walk down the street, you notice the man is following you. When you enter your house, the man just keeps walking down the street. You are relieved that it just seems like a coincidence. But it is not. The man knows your name. He knows that you have a contactless credit card, and he knows its number and expiration date. What did the man have in his briefcase? A $20 RFID reader and a small laptop. As he stood by you in the bus, his reader activated your contactless credit card and got it to disclose its number, expiration date, along with your name. As the man followed you on the street he noted the building you entered.

Is this the future? No, it is 2005, when all of the major credit card companies released new contactless credit cards built on RFID technology.

RFID is just a generic term for sending information over a wireless radio. Some say that the first RFID system was implemented during World War II to identify the flag of a particular airplane. However it was not until 1969 when the passive tag, which most people associate with RFID, was invented. A passive tag is a small circuit that has no normal power source. Instead, when it is brought close to a reader, the reader induces electricity to flow through the circuit, activating a very basic computer chip. The most basic RFID chips only reply with a static number; however more advanced chips available today are capable of encryption. Many of us already carry RFID cards. Many workplaces have issued the contactless cards because they are very convenient to open doors or turnstiles. Some cities, such as Boston, have implemented contactless transit payment cards. In addition, RFID chips don’t just need to be in credit card form factors. They can attach to a keyring or stuck to the back of a mobile phone.

All of the credit card implantations, branded as Visa PayWave, MasterCard PayPass, American Express Express Pay, Discover Zip, and Chase Blink all use the same over the air protocol. However, all use slightly different encryption and data standards. Furthermore, some card associations have even allowed different standards to be implemented under the same brand name.

One common misconception is that RFID cards can be read automatically and perfectly from across the room. This is not the case. In the real world, the tags cannot be generally read at a distance of more than one foot. In fact, as one implements more security, the effective read distance decreases. This is because tags with encryption chips require substantially more power than tags that simply return an ID. Thus these cards must be significantly closer to the readers. In order for an RFID card to be read from across the room, it requires a specialized antenna and a highly trained operator. We believe that consumers are not sufficiently aware of this information.

In addition, it is bad UI for the card to be able to be read from across the room. Many consumers are concerned about RFID tags being read without their knowledge. Combined with the difficulty in reliably reading cards surreptitiously in the deployed environment, we recommend that consumers always initiate the card read by holding the card to a reader, as opposed to attempting to read the cards through some sort of “portal.” In addition, this lets consumers choose which card to use. Thankfully this industry is currently requiring consumers to actively “tap”.

We believe that the credit card industry made a critical security miscalculation as it rolled out contactless payment cards in the United States. To understand this miscalculation, we need to take a look back at standard credit cards. Security in American credit cards was never baked into the card itself. [[1]](#footnote-1) In fact, the magnetic stripe of a credit card can easily be copied using a commercial magnetic stripe reader/writer available online for several hundred dollars. Instead, the card networks built security algorithms on the back end to monitor fraud both in real time and by locked down cards which exhibited suspicious behavior.

In Europe, the industry developed “EMV”-based “smart cards” and implemented it throughout the 2000s. Properly implemented chips enforce strong two-way encryption between the card and the card terminal, preventing the cloning of the card or the replay of transactions.[[2]](#footnote-2) In addition, in Europe, a PIN must be used with every transaction as a “second factor” of authentication. This second factor makes fraud harder because a thief needs to not only steal the card, but he or she must also observe the customer’s PIN. In countries in which “Chip and Pin” has been implemented, a “liability shift” has occurred to the non-EMV party.[[3]](#footnote-3) Essentially, where EMV is implemented, the liability shifts to consumers. In the United Kingdom, banks generally refuse to refund lost money if customers are duped into handing over their cards and disclosing their PINs.[[4]](#footnote-4) However, the United States provides no such exemption for acts of the cardholder.[[5]](#footnote-5) In addition, in the United States banks generally exceed the stationary liability protections into order to build the trust of the card holders.[[6]](#footnote-6)

The card industry chose to continue eating the fraud, rather than attempt to implement a secure standard. In a 2007 speech at the Visa Security Summit, Visa President and CEO John Phillip Coghlan’s speech did not talk about the need for his company to move to EMV, but on the need to build and maintain trust in the card system.[[7]](#footnote-7) While Visa and the card associations prefer better security, they were not willing to break their existing system or impair customer convenience. However, contactless cards require new point of sale equipment. We found that companies add contactless when they undergo their regularly scheduled point-of-sale replacement. Because the equipment is being replaced anyway, it would only be slightly more expensive to add EMV support for contactless cards at the same time. EMV would then slowly diffuse. Although it would not provide much additional protection until EMV is ubiquitous, the industry would be starting the transition now.

The card industry points out that this data is on the face of the card anyway. However, adding the wireless component changes things tremendously. While consumers had to worry about physical pickpockets, consumers are not accustom to being virtually pickpocketed. Furthermore, when a card is physically pickpocket, consumers have become aware of calling to deactivate it. When their card is digitally pickpocketed, there is no record. Furthermore, a photographic image of a credit card would certainly not be accepted for payment, while the contactless data of some credit cards would be accepted.

Europe’s contactless technology merely replaces a physical connection for a wireless one, providing significantly more secure than some contactless cards issued in the United States. In the United States however, the card associations retrofitted contactless technology into their existing magnetic strip infrastructure.

In a 2007 research paper several researchers in Massachusetts applied for and received RFID-enable credit cards.[[8]](#footnote-8) Before opening the envelopes, they read the cards with commercial RFID readers. All of the cards’ RFID responses contained forms of data which is usually found on the magnetic strip of the cards, including the cardholder’s name and credit card number (called the primary account number). When they opened the envelopes, they found that one of the cards simply transmitted the exact data that was on the card’s magnetic stripe. This same data which the industry prohibits the storage of could be read, over the air, a foot or two away from the card with any reader. Using this RFID data and the address printed on the envelope the researchers were able to order merchandise from a leading supplier of research electronics (who did not ask for the CVV2 code printed on the back of the cards). They could have also loaded this data onto another card’s magnetic stripe and used it at retailers. Or the researchers could have loaded the data onto an RFID token and pay for items wherever RFID cards are accepted. Other cards in their study dynamically changed the CVV1 code in the fake magnetic track according to a cryptography encoded counter. In this case the researchers would only be able to use each value once, in the order that each value was received from the card. However, in all cases the cards transmitted the cardholder’s name to whoever asked for it.

Card associations may argue at this point that many of the fraudulent transactions would be detected by their fraud monitoring system. They would also argue that consumers would not be liable for any purchases and those purchases are limited to a certain dollar amount. Furthermore they argue that this problem is limited to only a small subset of cards, since each bank, not the card association, can decide how much security to implement.[[9]](#footnote-9) However, even the idea that their names and in some cases, credit card numbers, are being broadcast to anyone in read range who asks for it is scary. Even if cardholders were not financially liable for charges, sorting out fraud on one’s account still takes some time. It also raises worried of identity theft, which the card companies would not be liable for. If one searches for “rfid credit cards” on a leading search engine, all of the results on the first page are negative, with all but one discussing security vulnerabilities. The security vulnerabilities made the mainstream news; the Today show ran a report criticizing the cards.[[10]](#footnote-10) Senator Charles Schumer (D-NY) asked the card industry to disclose that the card would be coming with RFID on the contract.[[11]](#footnote-11) The Consumerist blog, now owned by the non-profit that owns Consumer Report, ran a story on how to “De-RFID Your Credit Card.”[[12]](#footnote-12)

At a time when the credit card industry had to slowly replace much of its infrastructure to accept any form of contactless cards, it could have chosen to move up to the more secure EMV standard for contactless cards. When it was replacing half of its infrastructure, it could have also planned to change the other half. However, it short-sighted tried to retrofit contactless cards into the existing framework. The status quo of magnetic cards with only backend security was what consumers knew and accepted. However, when that information was being broadcast wirelessly to whoever asked for it, it changed the accepted norm. Certainly rumors that the cards could be easily read across the room did not help, but the possibility that their cards could be read from their wallets scared consumers. Compounding this, the industry made foolish mistake in issuing cards that broadcast the sensitive the magnetic track data in the rush to get the cards working. The card associations allowed these cards to be issued under their brand names. This led to a stream of news reports which showing how easy it was to not only clone a card but to make purchases with it. For consumers listening to the news reports, it did not matter if the bank’s fraud monitoring software detected the purchase after the fact or that consumers were not liable. The appearance that your money could be stolen by an attacker standing on the other side of the room with a laptop was deeply frightening.

RFID credit cards have the capability of being a great deal more secure if they are built on a standard similar to EMV. Consumers’ privacy would improve if the cards refused to release meaningful details to unauthenticated readers. If the card associations required a second factor of authentication, such as a PIN, the potential for fraud could drop dramatically. In addition, because the industry did not differentiate or explain to consumers, even sophisticated consumers, which technologies were being used, it gave all contactless payment methods a black eye. By obscuring the technology with brand names and failing to even prepare even a high-level animation of encryption, it lost the PR battle on security.

Furthermore, instead of fixing the problem, the industry further confused consumers by misrepresenting the security of the card. Rather than engage in an honest discussion about the security of their cards, they continued to claim that there were no issues. For example, the industry claimed that contactless cards were secure because they were only “active” during a transaction.[[13]](#footnote-13) While this is true, that electricity only flows through the card while the card is being interrogated by a reader, it is quite disingenuous, because the card can become active any time by placing it next to any RFID reader. While most consumers would not understand this distinction, it leads experts to be uncertain with the technology, leading them to communicate their uncertainty through the news media.

Since the initial roll out of RFID cards, banks have pulled back the issue of the cards in the United States. The authors were unable to even find, much less apply for a Chase “Blink” credit card. Searching for “blink” on Chase’s site led to a dead link.[[14]](#footnote-14) While attempting to apply for a PayPass MasterCard, we could see a selection of several cards, but we ran into errors when attempting to apply.[[15]](#footnote-15) Applying for a Visa PayWave card was partially successful.[[16]](#footnote-16) One bank told us that the offer was no longer available, but Wells Fargo appeared to be issuing PayWave cards.

## Moving Forward

One thing the payment industry could do is to adopt a UI convention for users to authorize payments. For example, a RFID credit card would not be active unless a user is depressing a button. If the button was located so that it was natural for users to touch it when holding the card, it would provide consumers with additional peace of mind that their card could only be read when they allow it. This further extends the convention of allowing the user to be in control. The credit card industry has just announced a conventional magnetic strip credit card with lights and buttons.[[17]](#footnote-17) However the first use of the card will be to not be to add security, but to let users select between paying with cash or reward points. Adding an RFID chip with an activation button would add peace of mind.

Additional, visible layers of security such PINs and physical inspection of the RFID card by the cashier, would increase security incrementally, but also slow down the convenience which RFID was supposed to introduce.

RFID technology can also be extended to payments using cell phones. NFC is the name given to truly integrating RFID receivers and transmitters into cell phones. This technology is currently a few years away as technical issues, particularly how to maintain security from the other processes running on the phone. Current trials just take the same RFID chip contained in actual credit cards and find some way of attaching it to a phone, such as a sticker or microSD card; there is no electrical connection between the RFID chip and the phone; the chip is simply attached to the phone.

1. http://www.nytimes.com/2010/10/17/business/17digi.html [↑](#footnote-ref-1)
2. http://www.cl.cam.ac.uk/~sjm217/talks/leuven07emv.pdf [↑](#footnote-ref-2)
3. https://mol.mastercard.net/mol/molbe/public/login/ebusiness/smart\_cards/one\_smart\_card/chip\_migration\_strategy/liability\_shift.jsp [↑](#footnote-ref-3)
4. http://www.timesonline.co.uk/tol/money/consumer\_affairs/article5575295.ece [↑](#footnote-ref-4)
5. http://www.law.cornell.edu/uscode/15/usc\_sec\_15\_00001643----000-.html [↑](#footnote-ref-5)
6. http://www.mastercard.com/us/personal/en/cardholderservices/zeroliability.html and http://usa.visa.com/personal/security/visa\_security\_program/zero\_liability.html [↑](#footnote-ref-6)
7. http://usa.visa.com/download/personal/security/visa\_securitysummit\_coghlan.pdf [↑](#footnote-ref-7)
8. Vulnerabilities in First-Generation RFID-enabled Credit Cards.

   Thomas S. Heydt-Benjamin, Dan V. Bailey, Kevin Fu, Ari Juels, and Tom OHare. In Proceedings of Eleventh International Conference on Financial Cryptography and Data Security, Lowlands, Scarborough, Trinidad/Tobago, February 2007. http://www.cs.umass.edu/~kevinfu/papers/RFID-CC-LNCS.pdf [↑](#footnote-ref-8)
9. http://www.nytimes.com/2006/10/23/business/23card.html [↑](#footnote-ref-9)
10. http://www.bing.com/videos/watch/video/smart-cards-are-quick-but-are-they-safe/6awros6 [↑](#footnote-ref-10)
11. http://schumer.senate.gov/new\_website/record.cfm?id=266771 [↑](#footnote-ref-11)
12. http://consumerist.com/2007/08/how-to-de-rfid-your-credit-card.html [↑](#footnote-ref-12)
13. Morea, Dom; "Contactless Payments: The 'Tipping Point' Is At Hand"; First Data; January, 2010 [↑](#footnote-ref-13)
14. <http://www.chaseblink.com/apply> 404 error on Oct 30 2010. [↑](#footnote-ref-14)
15. <http://www.mastercard.com/us/personal/en/aboutourcards/paypass/issuers.html> “The application you are requesting is currently unavailable.” On Oct 30 2010. [↑](#footnote-ref-15)
16. <http://usa.visa.com/personal/cards/paywave/issuers_offering.html> “Unfortunately, this offer has expired.” [↑](#footnote-ref-16)
17. http://www.nytimes.com/2010/10/22/your-money/credit-and-debit-cards/22cards.html?scp=3&sq=credit%20cards&st=cse [↑](#footnote-ref-17)