Switching Off Credit Card Fraud

The advent of contactless payment technology brings with it new opportunities for stealing information from a credit card without the owner’s notice. Consider the following scenario: a person with a credit card in a wallet is at a busy public place (say, on a train), and a miscreant with a tag reader is

within the read range of the card. The miscreant, after reading the card's tag without the owner's permission, would be able to identify the cardholder, steal whatever data was transmitted and potentially use that information to commit crimes. If a switch were added to deactivate the card when not in use, however, then fraudulent use of the cardowner's credit information could be reduced.

The type of information stored on a credit card—whether the traditional design with just a magnetic stripe or a contactless credit card with an embedded RFID chip—is specific to each card provider. Of course, the information on the credit card may not be complete enough to enable many kinds of fraud. A card is just one of many sources of personal information a thief can get, but thieves can do extra homework to fetch additional details of a particular cardholder.

Described below are some potential fraud scenarios facing major credit card vendors. The list indicates various types of fraud made possible by credit card information leaks, but such leaks may not be the sole causes.

• Opening a new credit card account using an owner's name, date of birth and Social Security Number, but with a different billing address.

• Asking for a change in the mailing address on the credit card account.

• Requesting additional credit cards.

• Counterfeiting debit cards to empty a bank account.

Compounding the problem, some credit card companies don’t require authorization for transactions under a certain value (e.g., below $25). In such a situation, the cardholder would unlikely be immediately aware of any purchases fraudulently made with that card. Even though credit card issuers typically exempt cardholders from any liability, fraudulent purchases could become increasingly worrisome to both card issuers and cardholders if they were to become more common. This is the main idea behind adding a switch to the credit card, as it would ensure that payments be made only when the switch is on, actively requiring the cardholder to authorize each purchase.

The antenna of a passive RFID tag is the powerhouse for the microchip that stores and transmits data. If a card were fitted with a switch to make or break the connection between the chip and antenna, the cardholder could squeeze the switch to turn on the card and wave it before a reader to make payments. Ideally, this feature should come as a default with the credit card, ensuring no data is captured from the card and no payment is made without the notice and permission of the owner.

Biometrics is another security technology the industry is looking into. Though more effective and secure, it would cost more to implement, and it is unclear if the cost incurred in implementing biometrics is worth it.

The future will accommodate both switch-on and biometric cards, but there is no such thing as a free lunch in this world. Every effort to improve security or customer service is an extra expense to card issuers, and these companies will have to pass that expense on to the end customer and/or the merchant. Since the cost incurred to implement biometrics is

high, the service provider may charge cardholders a fee for this value-added service. But for switch-on cards, the issuer may charge the end customer a small transaction fee, or the merchant may add a small percentage to the cost of the product. Customers willing to pay a higher amount may go for biometrics; for others, switch-on might be best.

Switch-on cards offer cardholders a number of benefits. Because switch-on cards are traditional smart cards with a built-in switch, cardholders should find them easy to use. The opportunity to steal information from such a card would be rare, granting cardholders a peace of mind.

Because switch-on cards can be manufactured cheaply, issuers can offer their customers a more secure card for little additional cost. And by reducing the fraudulent card use, switch-on cards could lead to better customer service because card issuers would have more resources (time, money and people) to focus on fighting the remaining fraud cases.

With the addition of a simple switch to activate or deactivate the RFID tag embedded in a credit card, contactless payments can be made more secure and user-friendly. This should boost consumer confidence in contactless payment cards, and increase their adoption and usage.

Prasad Paturi is an analyst at Wipro Technologies, a provider of integrated business, technology and process solutions on a global delivery platform. He participates actively in RFID initiatives at Wipro Technologies and has presented technical articles and innovative ideas on the application of RFID.

- ADVERTISE
- CONTACT

FOLLOW US ON

- Follow
- Follow
- Follow
- Follow

ABOUTCAREERSAUTHORIZED SERVICE PROVIDERSYour Privacy ChoicesTERMS OF USEPRIVACY POLICY