Dr Laura Poe

E: poelf@longwood.edu **T:** +1 804 356 0918 **T:** +1 434 395 2778
www.linkedin.com/in/laura-poe-phd

Adam Hoglund/Shutterstock.com

A case for biometric credit cards

Research Objectives

Laura Poe designed a case study to test the implementation of a biometric credit card, and its success at preventing fraudulent transactions.

Detail

Address
College of Business and Economics, Hiner Building,
201 High Street,
Farmville, VA 23909, USA

Bio
Dr Laura Poe is a professor of Information Systems and Cyber Security at Longwood University, Virginia, with research in areas such as biometrics, software quality, pedagogy, and project management methodologies. She has over 20 years of business experience and owns an IT consulting firm with numerous public and private sector clients.

References

Poe, LF, (2021) Case study: Empirical evaluation of a biometric credit card for fraud reduction. *Cybernetics and Systems*. doi.org/10.1080/01969722.2021.2005873

Personal Response

With NFC mobile payment apps becoming increasingly popular and secure forms of payment, what are the arguments for a biometric credit card?

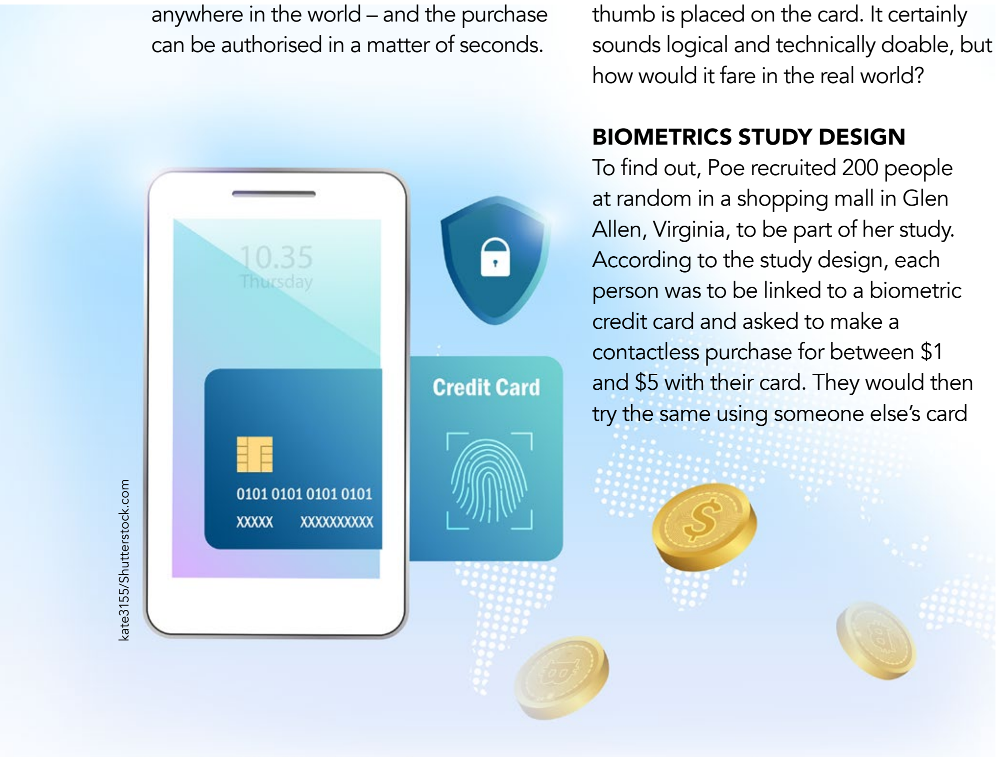
" Consumer research indicates the majority of debit and credit card users rely primarily on physical cards for making purchases in stores, and European markets show a growing trend for biometric cards. This trend is expected to continue despite the availability of cardless technologies. As fraud increases for online purchases, opportunities to leverage biometric capabilities can be further explored using digital biometric authentications. This research is the first biometric card study in the United States and indicates the increase in secure transactions using biometric authentications. "

A case for biometric credit cards

Credit card fraud is an unfortunate aspect of everyday life for banks and their customers, but it needn't be. PIN chips in cards offer some measure of protection but can be forgotten or stolen. There is an alternative: using biometrics on credit cards in the form of fingerprint identification. Dr Laura Poe, a specialist in cyber security, has conducted a case study with a biometric credit card and discovered that the technology has its promises but also its limitations.

Credit cards are an integral part of global retail, but their universality and practicality make them particularly attractive to fraudsters. Despite the banks' best efforts to prevent it, credit card fraud continues; it's an unfortunate part of their business, and the costs incurred are usually passed on to the consumer somewhere along the line.

Today's credit card is a marvel of technical ingenuity: a simple tap on a contactless terminal establishes a connection with the cardholder's bank – which could be anywhere in the world – and the purchase can be authorised in a matter of seconds.



kate3155/Shutterstock.com

But the process relies on the person holding the card being the registered card holder. In fact, there is a way to ensure the right person is holding the card – and it doesn't involve a 'PIN'.

Dr Laura Poe, a professor of Information Systems and Cyber Security at Longwood University in Farmville, Virginia, in the US, has designed a case study for a biometric credit card. The idea is simple: a credit card is registered to someone using their thumbprint; thereafter, the card will not work at a paypoint unless a matching thumb is placed on the card. It certainly sounds logical and technically doable, but how would it fare in the real world?

BIOMETRICS STUDY DESIGN

To find out, Poe recruited 200 people at random in a shopping mall in Glen Allen, Virginia, to be part of her study. According to the study design, each person was to be linked to a biometric credit card and asked to make a contactless purchase for between $1 and $5 with their card. They would then try the same using someone else's card to attempt a 'fraudulent' transaction. Poe's intention was then to compare the rate of any successful 'fraudulent' transactions using the biometric card with the current benchmark rate of fraudulent transactions using standard credit cards. Ideally, everyone would be able to register for a biometric card, every card used by the correct cardholder would be authorised, and every 'fraudulent' attempt would be rejected.

The first problem Poe encountered was registering users for the biometric card. In addition to the regular EMV 'chip', the study's biometric card used capacitive fingerprint sensing, which detects the pattern of ridges and valleys of a human fingerprint or thumbprint. This information is then stored on the card – it is not transmitted in any way, even to the cardholder's bank. However, the thinness of the card means the fingerprint sensor has a narrow 'detection distance', which limits its accuracy. It also has a thin protective coating, making it susceptible to damage through everyday use. Of the 200 people in the study, five were unable to register their thumbprints on the card, probably because their thumbprints were dirty which impeded the sensor. In a real-life scenario, this would prove frustrating for banks and cardholders alike.

FINGERPRINTS AND FRAUD PREVENTION

For a biometric credit card to be feasible, it first has to work as a method of payment. Anyone who's had a problem with their credit card at a busy till point would attest to that. In Poe's study, seven of the 195 cards used by the correct cardholder failed to authorise the transaction. Add those seven to the five who couldn't even register a card, and that's a total of 6% of participants who couldn't use a biometric card – not an encouraging statistic for banks which might be considering this technology.

The idea behind Poe's study was that cards registered by thumbprint would not work for anyone other than the card holder.

diyl3/Shutterstock.com

These initial limitations aside, the purpose of the study was to test the viability of biometrics in preventing credit card fraud. Of the 195 'fraudulent' attempts in Dr Poe's study, three succeeded. That may suggest a failure of the technology and a black mark next to the biometric card, but there's an encouraging story in the data. Three out of 195 is a fraud occurrence of 1.5%. Fingerprints are known not to be a failsafe method of identification – Poe quotes research showing that fingerprints have a standard error rate of 2.21% when used as a single mode of authorisation. This makes the 1.5% 'fraud' rate with the biometric card relatively healthy.

The biometric card really shone, though, when that 1.5% 'false positive' rate was compared to the rate of fraudulent use of standard credit cards. Poe used as a benchmark the rate of fraudulent card use in 2016 and 2017, immediately before her study. In both years, 32% of credit card transactions were fraudulent, a stark contrast to the 1.5% of 'fraudulent' transactions that slipped through the biometric card's authorisation process. Despite its limitations then, there is an argument for using biometrics on a credit card.

BIOMETRICS AND SECURE TRANSACTIONS

Biometrics – fingerprints and facial scans – are now the cornerstone of NFC (near field communication) mobile payment apps such as Apple Pay, Google Pay and Samsung Pay, but those apps still need to be linked to a credit or debit card. Embedded PIN chips offer some security, but PINs can be forgotten and stolen.

As Poe's study has shown, biometrics can offer an added layer of security against credit card fraud. The thumbprint scanning technology that banks would build into cards still has some way to go to be more accurate and robust, but overall, it seems the technology works.

Poe admits there's a crooked elephant in the room – fraudsters can still use a stolen or skimmed credit card for online transactions. But given how much banks lose to credit card fraud every year they should take a close look at any technology – especially one that can be relatively easily implemented – that ensures financial transactions are more secure and makes it harder for fraudsters to prey on the innocent.

> ***The biometric card really shone when its 'false positive' rate was compared to the fraudulent use of standard credit cards.***

Biometric cards could provide an important extra level of security for banks.

Miha Creative/Shutterstock.com

Vink Fan/Shutterstock.com