Proposal: 1818(AG67) Debit Card Interchange Fees and Routing

Description:

Comment ID: 158772

From: Reynold Schweickhardt

Proposal: 1818(AG67) Debit Card Interchange Fees and Routing

Subject: 1818(AG67) Debit Card Interchange Fees and Routing

Comments:

Date: Mar 23, 2024

Proposal: Regulation II: Debit Card Interchange Fees and Routing [R-1818]

Document ID: R-1818

Revision: 1

First name: Reynold

Middle initial:

Last name: Schweickhardt

Affiliation (if any):

Affiliation Type: Other (Oth)

Address line 1:

Address line 2:

City:

State:

Zip:

Country: UNITED STATES

Postal (if outside the U.S.):

Your comment: My name is Reynold Schweickhardt, and I have three decades of experience in the world of cyber security having served at the General Services Administration, and the US House of Representatives as a Senior Technology Policy Advisor. I have also served at the Government Publishing Office as the CIO and CTO. I am submitting this comment in opposition to the Federal Reserve´s proposed Rule II as I believe that it will weaken the ability of our financial institutions to protect against cyber breaches. Credit and Debit cards are compromised in one of two ways. First, the physical card is stolen or cloned using available information. Second, the card information is used without having access to the actual card which is a Card Not Present (CNP) transaction. Numerous data breaches have made significant amounts of Personally Identifiable Information (PII) available such as social security number, date of birth, mailing address, etc. which facilitates fraudulent transactions. Investments in better cyber security and fraud prevention are expensive but they weaken over time.

Standards evolve to mitigate new threats. In addition government regulations such as the EU's Revised Payment Services Directive (PSD2), especially its requirement for Strong Customer Authentication (SCA) increase the costs of compliance. Let's look at two examples of security measures. When holograms were first used to deter counterfeiting of physical cards the technology was very secure. Over time as hundreds of millions of holograms were applied to cards, the technology became cheaper and the software to duplicate banking holograms became simpler and more cost effective for fraudsters. To improve security standards such as Three-Domain Secure (3D Secure) were updated to streamline usability and added a biometric capability. .For example, the use of biometrics to secure financial transactions occurs when you call a bank or brokerage and they ask the consumer to speak a sentence which is subject to voice verification. Over time fraudsters will capture voice samples from phishing phone calls or social media video to reduce the effectiveness of this authentication method which will require further investments to maintain a required level of security. The risk of fraudulent card transactions is also mitigated using a set of data points to evaluate the risk of a specific transaction. Artificial Intelligence (AI) may allow fraudsters to more easily reverse engineer the vetting process and construct a fraudulent transaction framework which will evade existing protections. Of course, when detected the payment networks will expend resources to update their strategies to block that particular exploit. Continuing investments to maintain cyber security and fraud deterrence should not be starved by capping transaction fees arbitrarily.