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

Description:

Comment ID: 159865

From: Reynold Schweickhardt

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

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

Comments:

Date: May 13, 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): Fellow, Foundation for American Innovation

Affiliation Type: ()

Address line 1:

Address line 2:

City:

State:

Zip:

Country:

Postal (if outside the U.S.):

Your comment: Hardly a day passes without headlines highlighting a cyber-attack targeting the United States government, its major corporations, or individuals who sometimes lose their life savings with just a mouse click. Protecting this critical infrastructure from hostile adversaries and criminals is crucial for U.S. national security and personal privacy. Data protection poses significant challenges as the cyber battlefield constantly evolves, making it costly for companies to secure the highly sensitive information of millions of customers. Understanding these challenges, it is baffling to observe the Federal Reserve proposing a policy revision that appears to undermine the ability of financial institutions to safeguard the data of these companies' vast client base, potentially weakening rather than fortifying their protective capabilities. Logic would dictate that every government policy; whether local, state, or federal; would consider potential risks to critical infrastructure before implementation, as the consequences of a cyber compromise could be catastrophic. However, Regulation II; a recent

proposed rule from the Federal Reserve regarding bank interchange, or "swipe," fees; will place the processing networks utilized by banks and credit unions at even greater risk, exacerbating a problem of their own making. Banks and financial institutions constantly fight hackers and criminals who attempt to access bank accounts. These banks pay millions to protect this data, primarily from the revenue derived from interchange fees, the fees businesses pay when someone uses a debit card. Retailers, however, detest the small fee and went to Congress to restrict it. In 2011, the Fed, for the first time, implemented a rule that reduced the interchange fees banks were permitted to charge. This rule, known as the Durbin Amendment after its sponsor Sen, Dick Durbin (D-IL), capped these fees at .21 cents per transaction, plus an additional .05 percent of the total sale. The Fed at the time also permitted a .01 cent per transaction fee to cover the cost of "fraud prevention." The strongest advocates of this original rule were large merchant retailers (think Walmart and Amazon), and they exploited their outsized influence in Washington, DC, to mandate the Fed to take this course of action. The rule ended up hurting consumers. Retailers who pledged to reduce prices if the fee was price-capped never did. Banks and credit unions were forced to reduce product offerings to clients, such as free checking and airline miles, due to loss of revenue. Large merchant retailers saw a hug uptick in profits; some estimates indicated upwards of $100 billion; while offering consumers little or no price relief. However, perhaps the most concerning consequence has been the surge in fraud claims. Since 2011, fraud claims have increased by more than 60% - with most of those costs being born by the same financial institutions negatively affected by the price cap imposed by the Fed. But like a scene out of a bad movie, the Fed is now proposing further reducing interchange fees by an additional 30%. 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 to access 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 a person's Social Security number, date of birth, and mailing address, which facilitates fraudulent transactions. Better cyber security and fraud prevention investments are expensive, but they weaken over time. Standards evolve to mitigate new threats, which change daily, and financial institutions must make investments to counter them. Regulation II risks making these companies unable to make the updates they need to keep their customers' data security. Continuing investments to maintain cyber security and fraud deterrence should not be starved by capping transaction fees arbitrarily. As such, the Fed should reconsider Regulation II. Reynold Schweickhardt is a fellow at the Foundation for American Innovation, and former Director of Technology Policy at the U.S. House of Representatives.