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

Description:

Comment ID: 159873

From: Sultan Meghji

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: Sultan

Middle initial:

Last name: Meghji

Affiliation (if any):

Affiliation Type:()

Address line 1:

Address line 2:

City:

State:

Zip:

Country:

Postal (if outside the U.S.):

Your comment: As the former Chief Innovation Officer of the Federal Deposit Insurance Corporation (FDIC), I understand the critical role that community banks and credit unions play in our financial systems. These small but vital actors are indispensable for many Americans in accessing needed financial services such as checking and savings accounts, access to credit and mortgages, and the ability to utilize typical financial products to pay their bills. They often have more personalized relationships with their clients, as they are members of their communities. This mutually beneficial relationship gives access to the underserved and has proven for decades to be the most effective job creator by facilitating the creating new business, and helping average Americans achieve their dreams. Unfortunately, community banks and credit unions have been under ever-increasing financial pressure over the last three years. First, higher interest rates; now hovering around 7% for a 30-year fixed

mortgage; have substantially reduced overall mortgage origination, and despite small glimmers of hope on the horizon for a reduction in inflation, the Fed has laid out no clear path for a corresponding rate cut. Second, ost COVID commercial real estate vacancy increases have exposed many small lenders to the risk of defaults in that economic sector, as small banks hold nearly two-thirds of all commercial real estate loans. Recently, fears of more bank failures have emerged with a variety of groups suggesting potentially hundreds of banks are now at risk of failure. And now a third significant stressor is coming - A newly proposed Federal Reserve rule to further limit debit card interchange fees; the processing fees corporations pay to have debit cards processed in their stores; will only worsen this situation, exacerbating financial institutions' current financial struggles. For the last decade, we have watched these pressures cause Banks and Credit Unions to restrict their spending around technology, especially cybersecurity. In 2011, as a part of the Dodd-Frank Wall Street Reform Act, Congress required the Federal Reserve to cap this swipe fee for the first time. At the time, several Fed Board of Governors members expressed serious concern regarding the potential negative consequences of this action. Still, they were required to act due to the congressional mandate, so they did so begrudgingly, acknowledging that this action would likely have unintended consequences. The results for the banking industry proved predictable. Banks and credit unions had no choice but to fundamentally alter their client relationship matrix and significantly curtail their product offerings. They eliminated many free checking and reward programs that customers enjoyed. ATM and overdraft fees increased, and higher minimum balance requirements became the new normal. All these actions became essential for protecting their solvency, replacing the revenue streams that the new Fed swipe fee edict restricted. In 2012, the Government Accountability Office reported that, over the previous six years, "the number of incidents reported by federal agencies to the federal information security incident center has increased by nearly 680 percent." Many banks that wanted to bolster their cybersecurity operations to reflect these new and emerging threats found themselves unable to do so. Understandably, some estimates indicate that this Fed swipe fee policy created more than $100 billion in losses for them over the last ten years, with a Mercatus Center study finding that the Durbin amendment reduced nearly three-fourths of all financial institutions' earnings. With the Fed effectively restricting their cybersecurity budgets, it should not surprise anyone to hear that banks faced significant hackings nearly immediately after this swipe fee cap was implemented, including simultaneous outages in September 2012 due to a coordinated denial of service cyberattack. Instead of recognizing the negative consequences incurred by this regulation, the Federal Reserve may now worsen the problem. On May 12, the Fed will close its comment period for a November notice of proposed rulemaking to further restrict the debit card interchange fee by over 30%. This time, the Fed is taking this action despite no congressional requirement. This raises the question: Does the Fed not realize that cyber threats remain a clear and present danger to our financial system and that doubling down on this failed policy will increase the prevalence of dangerous hackings in our financial system? In the first two quarters of 2023, the Federal Trade Commission Sentinel Network received over 38,000 reports where fraudsters used a debit card as a payment method. In 2018, losses to banks from fraudulent debit card transactions were more than 1 billion dollars alone, not including the losses absorbed by bank customers. This fraud happens in many ways; skimming devices, the purchase by malignant actors on the Dark web of large volumes of credit and debit card data combined with personal information, and "card not present" (CNP) transactions, which are online or mobile transactions, and are increasing at an alarming rate due to the ingenuity of hackers. The adversary takes an "all-of-the-above" approach, from the mundane to the complex, to breach financial systems, often marrying that sensitive data with publicly available information from social media and other platforms to create a "profile" that mimics the purchasing habits of legitimate users to mitigate fraud prevention efforts. Financial institutions are intimately familiar with the workings of these criminal organizations and utilize Artificial Intelligence (AI) to help detect anomalous patterns and highlight riskier transactions. Unfortunately, fraudsters also use AI and have methodically recruited IT professionals with cyber, reverse engineering, and offensive operations skills over the last four years to stay on par with financial institutions' newer, more secure systems. This is just the current state of play. However, even more significant threats are on the horizon, making it even more difficult for banks and credit unions to secure their transaction networks. Generative Artificial Intelligence (GenAI) is in the early stages of development but represents a significant threat to cybersecurity as it matures and takes shape. Quantum computing is not far behind. Financial institutions and their executive teams are keenly aware of the daunting challenges these threats pose. A recent report by KPMG revealed that 81% of the 100 senior banking executives surveyed expect

cyber threats to increase. Yet, over a third (34%) said their bank is not investing enough in cybersecurity protection. Nearly half indicated their banks are ill-equipped to protect customer data during a cyberattack. The report from KPMG is sobering and clarifies that industry leaders recognize the problem but that regulations have gotten in the way of their ability to address it. Between 2021 and 2023, financial services institutions reduced their spending on cybersecurity by nearly 33 percent. While there are no doubt multiple reasons behind this overall reduction, one thing is clear; reduced revenue from debit card interchanges has hindered the ability of banks and credit unions to respond to the increasingly complex cybersecurity threat matrix. The main danger lies with small and medium-sized banks and credit unions, which don't command even a fraction of the market share yet, at the same time, perform vital services to local communities throughout the country. These organizations are already massively underspending in technology, especially cybersecurity. Increased costs for cyber plus reduced revenue from interchange fees equals potential grave consequences for small financial institutions. This is creating a new systemic pressure on the US Banking System The Federal Reserve did not take this information into account when drafting its updated rule on interchange fees. My experience at the FDIC gives me some insight into the decision-making process of federal regulatory agencies, and my conclusion is this: the Fed, responding to political pressure, made a hasty decision without considering all the facts and consequences of a further reduction in revenue for banks and credit unions. This proposed rule is bad policy, and the Fed needs to rescind it.