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

Description:

Comment ID: 158521

From: John Jay College of Criminal Justice, Adam Wandt

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

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

Comments:

Date: Feb 12, 2024

Proposal: Regulation II: Debit Card Interchange Fees and Routing [R-1818]
Document ID: R-1818
Revision: 1
First name: Adam
Middle initial:
Last name: Wandt
Affiliation (if any): John Jay College of Criminal Justice
Affiliation Type: Educational (Edu)
Address line 1: 524 W 59th Street
Address line 2:
City: New York
State: New York
Zip: 10019
Country: UNITED STATES
Postal (if outside the U.S.):

Your comment: I am writing to urge the Federal Reserve to defeat Proposed Regulation Rule II imposing further government-established price controls on debit card transactions fees. My name is Adam Scott Wandt, I am an Associate Professor of Public Policy and Vice Chair for Technology in the Department of Public Management at John Jay College of Criminal Justice. I am a faculty member in John Jay's graduate program in Digital Forensics and Cyber Security and publish in academic and professional journals on issues involving cyber security. Much has been written about the financial impact of rules establishing price controls on interchange fees for debit card transactions (the fee paid to process debit cards), but not as much has been written about the impact they would have on cyber security. My primary concern with Proposed Rule II is that revenue derived from interchange transactions is invested to protect the American people's data and financial privacy. We know that the first iteration of instituting price caps on interchange fees forced financial institutions to either raise consumer fees or lose significant revenue. If it's allowed to move forward, the second iteration of this rule will cause card processors to lose even more of the revenue they depend on to protect the American people from hackers, thieves, and regimes that undermine the U.S. government. The personal financial data of the American people is a honey pot for hackers. Director of the Federal Bureau of Investigation Christopher Wray warned that Congress hackers backed by the Chinese government are strategically positioning themselves within critical infrastructure systems to "wreak havoc and cause real-world harm to American citizens and communities." Mr. Wray said that the "cyber onslaught" of Chinese hackers "goes way beyond pre-positioning for future conflict" because the hackers are "actively attacking" U.S. economic security every day, engaging in "wholesale theft of our innovation and our personal and corporate data." Moreover, just last days ago, Attorney General Merrick B. Garland said that the Justice Department "disrupted a PRC-backed hacking group that attempted to target America's critical infrastructure utilizing a botnet." He continued by assuring the public that "the United States will continue to dismantle malicious cyber operations; including those sponsored by foreign governments; that undermine the security of the American people." Depriving

businesses that deal with the American people's sensitive financial information of the revenue they need to fund their cybersecurity operations would run counter to that aim. American consumers deserve and need the highest level of protection available. It is unrealistic to believe this protection can come at an interchange fee rate that is cut even more than it is already. The threats we face in the digital realm are evolving and becoming more sophisticated. Our financial institutions must remain adequately funded to innovate and strengthen cybersecurity measures. We cannot afford to compromise on the safety and security of the American people's financial data. I urge the Federal Reserve to consider these factors carefully and to reject Proposed Regulation Rule II, in favor of strategies that ensure robust cybersecurity measures are maintained and enhanced.