Testimony of Steve Mathison, SVP of Network Relations, First Data Corporation
Before the House Committee on Agriculture, Subcommittee on Nutrition
June 8, 2017

Good morning, Chairman Thompson, Ranking Member McGovern, and members of the Committee.

My name is Steve Mathison, and I am Senior Vice President of Network Relations at First Data Corporation. I am pleased to be here today on behalf of First Data, and I appreciate the opportunity to share with you our perspective on the modernization of the Supplemental Nutrition Assistance Program (SNAP) and efforts to make it more efficient and effective for the millions of Americans who rely on these benefits in their everyday lives.

After providing an overview of First Data's role in the SNAP system, I will focus my comments on three primary areas: (1) technological availability; (2) payments security; and (3) increased competition.

First Data sits at the center of global electronic commerce. Founded more than 40 years ago, First Data serves approximately 6 million business locations and 4,000 financial institutions around the world. We are one of the largest retailer payment processor and bank issuer processors in the world, enabling businesses to accept electronic payments, helping financial institutions issue credit, debit, and prepaid cards, and routing secure transactions between them. In 2016, we powered 88 billion global transactions, or more than 2,800 transactions every second of every day, totaling $2.2 trillion per year, which is equivalent to nearly 10% of U.S. Gross Domestic Product. In addition, First Data owns the STAR debit network, with over 1 million point of sale (POS) and ATM locations nationwide.

Overview of SNAP Payment Processing

In order to consider our comments in the appropriate context, it is important to understand the basic transaction flow for a cardholder using an electronic benefit transaction (EBT) card. Technology providers like First Data enable commerce by facilitating the transaction processing connections between retailers, networks, and payment card issuers. Behind the scenes, the process is broken down into two distinct transaction processes: authorization and settlement.

When a consumer uses a payment card to purchase goods, the retailer must obtain authorization for the purchase from the bank that issued the card. This authorization is confirmation that the consumer's account is in good standing and that there are sufficient funds available in the consumer's account to cover the purchase. And, if the authentication process includes the consumer's Personal Identification Number (PIN), that PIN is also validated by the issuer to ensure the legitimate consumer is the one attempting the purchase. In the case of SNAP EBT cards, the state holding the SNAP funds is considered to be the card issuer (and the state may contract that service out to a third party to manage the accounts on the state's behalf). The authorization is, essentially, a request to make funds available to the

retailer for the purchase.

If the authorization request meets the card issuer's requirements, and the PIN passes the issuer's PIN validation algorithm, a reply is returned to the retailer, via the retailer's payment processor, indicating that the request has been approved. If the authorization request does not meet the card issuer's requirements, or if the PIN validation is unsuccessful, the retailer is informed that the requested transaction has been declined.

The final step is the "settlement" process in which funds are received in aggregate from the card issuer (i.e., the state holding the EBT account) for all approved SNAP transactions occurring at all retailers accepting SNAP cards during that business day. Funds are then separated into the proper amounts for each respective retailer, and those funds representing all the approved SNAP transactions processed at a retailer's location are then transmitted to each retailer's bank account.

First Data's role in the SNAP system is to enable retailers to accept SNAP cards in their stores and ensure that each SNAP transaction is routed to the appropriate state for both the authorization and settlement processes: we authorize SNAP transactions for retailers accepting the cards, our STAR network also authorizes cash transactions in authorized locations for SNAP cardholders, and we settle the accounts for our retail customers for approved SNAP transactions that have occurred during the day.

Technology Improvements

As we think about the future of SNAP and the desire for a more modern system, technological availability comes immediately to mind. In the bank-issued card world, the infrastructure supporting the payments rails is subject to a series of rules and agreements to ensure that outages do not regularly occur.

Quest is the network that provides the operating rules that govern the distribution of government benefits including SNAP. Quest is governed by the National Automated Clearing House Association and encourages that government entities incorporate the Quest rules in their contracts with third party entities used to distribute benefits.

There are differences in how the oversight and controls for the bank-issued credit and debit cards are managed by global payments networks such as Visa or MasterCard versus how the oversight and controls are managed relative to the Quest network. For example, in the case of a Visa or MasterCard network, those two entities take an active role in ensuring that there are service-level agreements and sufficient technology infrastructure across the entire payments eco-system so that if a systems issue were to occur at a payment processor, the network, or at a financial institution that issues the cards, there are redundancies and business continuity plans to ensure that commerce is not disrupted. The lack of similar service standards and requirements for SNAP processing leads to the SNAP cards not working for large numbers of cardholders on a fairly frequent basis. As you can imagine, system-wide outages have negative

impacts on SNAP recipients by reducing their access to necessary purchases, causing frustration for retailers and cardholders alike, creating extra inefficiencies and costs, and undermining confidence in the program.

We think this is an area that the federal government should explore. Adding baseline standards not only provides an incentive for state agencies and SNAP providers to improve, it will also lead to increased systems availability, lower costs, and an overall improvement in throughput which ultimately will ensure the consumers standing in the checkout lanes can get their benefits when they need them.

Payments Security

Additionally, we think the SNAP program could benefit from taking a more modern look at payments security. When we think about payments security in this space, we generally are thinking about criminals attempting to compromise the card number. This can occur when a criminal steals the card information at the card swipe, or steals it by hacking into the systems where card information is stored. The stolen card information is then used to create counterfeit cards by encoding the card information onto the magnetic stripe of generic plastic cards. Or, criminals can use that card number online to make unauthorized purchases.

The traditional bank-issued debit and credit cards have been undergoing a transition from relying solely on the magnetic stripe on the back of the card to including a more secure chip that interfaces with a point of sale terminal for the transmission of transaction data. The chips have microcomputers in them that are able to produce dynamic cryptograms and algorithms that make the cards much more difficult to counterfeit than the card data from a magnetic stripe, which holds only static information. Since the chip data is very difficult to reproduce, this lowers the incentive a criminal might have to steal card information – since the stolen card data from a chip card is very difficult to monetize via the conventional process of creating a counterfeit card and making fraudulent purchases, there is little to no benefit from stealing the card data in the first place.

However, chip technology, while certainly more advanced than the magnetic stripe, is not a panacea for all card fraud; its benefits are limited to stopping counterfeit card production.

There is an unresolved industry question about whether state agencies should be prescribing chip technology for SNAP cards. From what we see across our retailer base, the broader government benefit card environment has very small amounts of counterfeit fraud (i.e. stealing the card information from a legitimate SNAP card, reproducing a duplicate of the original card, and using that duplicate to make purchases), because PINs are required for all government benefit cards, including SNAP cards. In other words, First Data isn't seeing much counterfeit card production in the government space; and since adding a chip primarily only addresses counterfeit cards used at the physical point of sale, we don't believe that prescribing chip implementation in SNAP cards will create material fraud reductions or cost savings across the SNAP payments ecosystem.

However, the reason the counterfeit fraud is low is because each SNAP recipient must use two-factor authentication to make a SNAP purchase – the cardholder must present his/her physical card AND must enter a PIN for each and every transaction. And because the two-factor authentication is an effective method for preventing fraud, First Data believes PINs should continue to be mandatory.

The Payment Card Industry Data Security Standard (PCI DSS) governs data security for credit and debit cards, and PCI requires, for example, a certain level of hardware security. For example, PIN pads today self-destruct if anyone tries to tamper with them or even open them to access their internal technology.

When a consumer enters a PIN on a PIN pad at a retailer location, the PIN is encrypted, leading to a much more secure transaction.

Several years ago, only about half of the 8-10 million retailers that accept credit and debit cards had PIN pads. With the migration to chip cards, however, many retailers have decided to upgrade their point of sale terminals to be able to securely accept and process the chip card that's presented.

It's now fairly standard in the industry for a retailer to have a standard PIN pad, because the keys for the security chips are also in the PIN pads.

As more retailers move into the online grocery space – where a traditional PIN pad is not present because the consumer is transacting from his/her computer or smart phone – we think it's important for government agencies to explore enhanced security.

Specifically, we recommend that the federal government explore requiring that SNAP transactions made online or in an eCommerce environment (i.e. the consumer does not transact within the retailer's physical store, but rather initiates the transaction remotely via a computer or a mobile phone) should have two-factor authentication. Two-factor authentication involves data other than simply authenticating that the individual attempting the transaction has an account number.

In addition to something the individual *has* (such as their SNAP card), the second factor of authentication typically takes the form of either something the individual *knows* (such as a PIN or the answer to security questions) or something the individual *is* (such as fingerprint scans).

Additional forms of cardholder authentication are key in order to enable SNAP redemptions for emerging opportunities such as online grocery shopping and remote ordering for in-home delivery. Fraud in the eCommerce space is much higher than the physical point of sale. As such, having a way to keep fraud rates manageable and low in these higher-risk transactions will be an important factor in keeping SNAP funds flowing as benefits to recipients rather than fraud losses.

Increased Competition

Finally, as we think about a sustainable future of SNAP that leads to positive cardholder experiences, we believe the government should be taking steps to encourage competition among the payment processors that contract with state agencies to manage the state's SNAP programs.

Currently, there are few processors that occupy this space. And while these processors compete with each other as they bid to be a state's SNAP contractor, generally the state selects only those contractors with the lowest cost bids, which creates a cost prohibitive environment for other processors to try to enter the market.

While there is limited competition during the bidding process, once a contractor wins a bid from a state, that processor effectively becomes a monopoly for how that state's SNAP transactions must be processed. Retailers that wish to offer SNAP acceptance in their stores *must* process with that contractor. There is no alternative; the retailer must simply acquiesce to the demands of the contractor. This has become especially problematic because of the introduction of new fees by the dominant processors in an effort to supplement the thin-margin bids used to win the state's SNAP contract. These fees impact the retailers accepting the cards and the retailer processors like First Data who route the transaction from the retailer location to the network and the state.

Retailers and merchant processors are in a tough situation where they are essentially forced to accept any fee that is assessed by these state processors because there is no other option for processing a SNAP transaction for that state.

Generally, we believe the federal government should take the position that the imposition of processing and transaction fees for state processors is prohibited. Simply put, charging the retailers a fee for allowing a SNAP beneficiary to buy groceries at their store is unfair. The imposition of these fees could have the chilling effect of retailers deciding to curtail or cease acceptance of SNAP benefits altogether.

Or, as an alternative, we suggest the creation of a mechanism for a retailer to negotiate and/or process their SNAP transactions with a competing contractor for a given state. If fees must be imposed, they could be market-driven, competitive, and negotiated rather than imposed unilaterally.

In conclusion, as the electronic payments system continues to adapt to respond to innovative technologies as well as growing cyber threats, we commend the Committee for exploring ways to modernize the SNAP program. Clearly many Americans rely on the program to improve their lives, and we believe these Americans should have the same positive experiences when transacting with SNAP cards as others do when transacting with traditional bank-issued credit and debit cards.

As one of the entities that provides the infrastructure used to transport payment card data securely and efficiently along the payments rails, we appreciate the opportunity to provide our perspective on modernization efforts and look forward to keeping an open dialogue with the Committee members as new ideas are brought to bear.

Thank you, and I will be happy to answer any questions you may have at this time.