December 13, 2013

Adam Sedgewick
National Institute of Standards and Technology
10 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

RE: Preliminary Cybersecurity Framework

Dear Mr. Sedgewick:

First Data appreciates the opportunity to respond to the NIST Preliminary Cybersecurity Framework ("Framework").

We applaud and welcome NIST's efforts in suggesting best practices for organizational adoption to address cyber security concerns. We also acknowledge NIST's challenges in creating a suite that is effective but flexible enough to help critical infrastructure owners and operators – of varied size and function - identify, assess and manage cyber risk.

However, our experience suggests that the Framework is too restrictive in the proposed collection, use and dissemination of Personally Identifable Information ("PII") in Appendix B's Governance Category beginning o page 26. Thus, found below are: (1) brief summary of First Data and its unique place within the Financial Services Sector; (2) specific concerns with the PII language found within the Governance Category; and (3) suggested alternate language for adoption within the Category.

I. FIRST DATA SUMMARY

First Data is a leading processor of electronic payment transactions. As a payment processor, we enable businesses to accept electronic payments for goods and services. Our systems must connect retailers to payment networks and to card-issuing financial institutions. Transaction data is shared among these parties – in a secure environment – in order for consumers to freely transact at brick and mortar locations, over the Internet, or via mobile devices. Despite having n direct contact with the consumer, there are various services we provide our customers for which the collection, use and, in some cases, distribution of PII is an absolute necessity.

We may collect, transmit or use PII in order to effectively perform some of the following services:

- Process transactions: effective payment processing requires sharing of certain information with entities along the payments value chain. Some transactions (e.g., Internet-based transactions or those initiated over the phone) may require additional data points so that processors and payment networks can minimize fraud and retailers can negotiate better interchange rates.

- Fraud prevention: identifying and stopping potential fraud across multiple cards, financial institutions and point of sale access points are integral components of payment processing. Our fraud prevention products rely on certain personal data to verify the appropriate individuals authorized to transact on specific accounts.

- Chargebacks and returns: chargebacks and returns can be initiated by consumers when they don't receive a good or service purchased or the good/service is faulty. Personal data is often accessed in chargeback or return scenarios to match the returned item with the appropriate purchaser.

- Check verification: personal data may be accessed at the point of sale to match check writers with negative history such as check kiting and check fraud. These services can help merchants evaluate the likelihood that check will be returned and protect themselves against fraud or purchases made with insufficient funds.

In addition to processing transactions for merchants, First Data also provides back-office services to financial institutions that issue debit and credit cards. Our services to these financial institutions may include maintenance of cardholder accounts, authorizing and posting of consumer transactions, generating and printing cardholder statements, card embossing, and fraud and risk management services. Here are just few examples of how these services might access PII:

- New credit card applications: we use personal data to verify application information such as employment, name, address and phone number or fill in missing information o the credit application.

- Stolen cards: if consumer reports stolen card, we rely on "out of wallet" information to ensure that it is the victim calling rather than a criminal trying to reactivate the card using information found in a wallet. We d this by asking questions that only the true cardholder should know; these answers are found behind the scenes by tying personal data to various public real estate data.

- USA PATRIOT Act requirements: personal data may be used to confirm the identity of individuals attempting to open an account at a financial institution. It is a USA Patriot Act requirement to obtain certain minimum information from a new customer and to verify that information in order to detect and deter criminal activities, such as money laundering and terrorist activities.

In performing these types of services, we have a core responsibility to our clients to ensure that every transaction we process and every function we perform is done so safely, securely and reliably. To meet that obligation on a daily basis, we employ a comprehensive and evolving security strategy.

Our Chief Information Security Officer (CISO) leads a highly-trained and full-time information security team that, among other things, directs our corporate participation with leading organizations, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) and its Threat Intelligence Committee. As you may know, the FS-ISAC routinely shares risk mitigation best practices to address vulnerabilities and recent cyber attacks.

First Data is also eligible to participate in FinCEN's granting of the Safe Harbor, LLC-- Section 314(b) of the USA PATRIOT Act providing financial institutions with the ability to share information with one another, under a safe harbor that offers protections from liability, in order to better identify and report potential money laundering or terrorist activities--for our prepaid and Online Banking lines of business. Here, we are working on the details of how information can be shared and consumed via the Safe Harbor, LLC by preventing the funding of known "money mules" and other criminal actors who use prepaid cards to move money.

Further expected benefits of participating in 314(b) sharing program are helping financial institutions enhance compliance with their anti-money laundering/counter-terrorist financing (AML/CFT) requirements, most notably with respect to:

- Shedding more comprehensive light upon overall financial trails, especially if they are complex and appear to be layered amongst numerous financial institutions, entities, and jurisdictions.
- Building a more comprehensive and accurate picture of a customer's activities where potential money laundering or terrorist financing is suspected, allowing for more precise decision-making in due diligence and transaction monitoring.

- Alerting the contacted financial institution to customers about whose suspicious activities it may not have been previously aware.
- Facilitating the filing of more comprehensive and complete SARs than would otherwise be filed in the absence of 314(b) information sharing.
- Aiding in identifying and collectively stemming money laundering and terrorist financing methods and schemes.

In addition to our participation in industry-specific organizations that establish leading practices, standards, and risk mitigation tactics, First Data works closely and cooperatively with federal departments and agencies, including the Department of Homeland Security, the U.S. Secret Service, and the Federal Bureau of Investigation.

Our information security practices have been and remain a top priority, which we enhance o an ongoing basis to meet business needs and emerging threats. We view our responsibility on this topic very seriously. In fact, our corporate board of directors and audit committee receive regular updates on these practices.

From a regulatory perspective, our company is supervised and examined by the Federal Financial Institution Examination Council (FFIEC). The FFIEC regularly examines and monitors our cyber security practices, including compliance with a layered approach to managing information security risks.

II. SPECIFIC CONCERNS WITH THE PII LANGUAGE FOUND WITHIN THE GOVERNANCE CATEGORY

We have two concerns with the Governance Category's language in subsection [i] suggesting internal adoption of cyber security procedures that "provide notice to and enable consent by affected individuals regarding collection, use, dissemination, and maintenance of PII."

First, as illustrated above, we come into contact with consumer PII on daily basis. However, we have no direct relationship with consumers. Thus, implementing an enterprise-wide policy whereby we can provide notice to and/or collect consent from consumers is impractical. Furthermore, consent requirement would not be appropriate for company like First Data, since an integral component of the services we provide our clients is fraud prevention. It is not difficult to imagine a scenario where a criminal attempting to perpetrate fraud would merely withhold consent in order to more freely conduct illicit activity.

Therefore, in order for companies like First Data to provide our clients with effective, safe and reliable payments processing and back-office support, many of which are inherently geared toward preventing fraud, we must not be subject to overly burdensome restrictions on the collection, use, dissemination and maintenance of the PII we acquire or to ill-fitting requirements to obtain consent from consumers with whom we have no relationship.

Additionally, placing such notice and consent restrictions on the collection and use of PII seemingly overextends the Civil Liberties protection aimed at by Executive Order 13636. For instance, in the course of our fraud prevention activities, we may acquire PII of suspected criminals and cyber attackers. We would then partner with various federal and state law enforcement agencies to inform them of the suspected criminal activity—and the acquired PII-- we receive. NIST's requirement for us to gain consent before collecting, using or sharing the PII gained through attempted or suspected criminal activity and/or cyber attacks seems counterintuitive. It appears to place the criminals' "civil liberties" ahead of consumer protection and the need for the private and public sector to partner to address and combat such attacks in concert with each other.

III. SUGGESTED ALTERNATE LANGUAGE

As illustrated above, we cannot practically effect, administer or enforce transactions initiated by consumers or protect against or prevent actual or potential fraud, unauthorized transactions, or cyber attacks with the preliminary draft language in subsection (i). We propose the following as practical alternative:

Replace subsection (i) in its entirety with the following:
Organizations should identify policies and procedures that address privacy or PII management practices. Organizations should assess whether or under which circumstances such policies and procedures:
"i) **ensure the privacy, security, and confidentiality of personal electronic records; protect against any anticipated vulnerabilities to the privacy, security, or integrity of sensitive personally identifying information; and protect against unauthorized access to or use of sensitive personally identifying information that could result in substantial harm or inconvenience to any individual."**

Adopting such language allows for the substantial protection of PII but provides more flexible approach that is necessary for effective payments processing, fraud prevention and ensuring that alleged cyber attackers' civil liberties are not placed above the need to communicate and work hand-in-hand with various state and federal law enforcement agencies in deterring fraud and cyber attacks.

CONCLUSION

We believe that the financial services sector already provides a gold standard of data protection that can be modeled by other sectors in the United States. Further, we take our responsibility to protect data very seriously and thus applaud NIST's efforts to develop best practices that a variety of organizations may adopt to effectively safeguard critical infrastructure and consumer data. We also appreciate the challenge of creating and implementing policies and procedures that are flexible enough to be adopted by organizations of differing size and needs.

However, we have grave concerns that the current language requiring notice and consent in order to use, collect or share PII could lead to severe unintended consequences that undermine the very intent of the cybersecurity framework. Not the least of those unintended consequences would be an inability for payment processors to detect and deter potential and actual fraud as well as hampering the flow of information between the public and private sector to respond to and protect against cyber attacks.

We appreciate the opportunity to provide our comments to you on such an important issue, and we are happy to answer any further questions. Please don't hesitate to contact me if you have any questions or concerns or would like additional information.

Sincerely,

Joe Samuel
Senior Vice President of Global Public Affairs
(303) 967-7175
Joe.samuel@firstdata.com