October 11, 2013

Subject: Comments to the Payment System Improvement – Public Consultation Paper

To The Federal Reserve Banks:

Thank you for the opportunity to comment on the Payment System Improvement Public Consultation Paper. I would like to respond specifically to your request for gaps and opportunities that were not identified and outline a strategy and tool that will help shape the future of the U.S. payment system.

A crucial gap in the U.S. payment system is the lack of a **standardized unique identification process** that prevents the use of multiple, duplicate and synthetic identities by individuals to commit fraud. Also missing is a **new customer identifier** which ensures that each unique customer is linked to only one identity, regardless of the payments network used. Without unique identification and such an identifier, the proliferation of payment networks, despite offering greater options for end users, will result in a growing maze of avenues for fraud, money laundering and financial crimes.

Granted, the USA PATRIOT Act requires the implementation of customer identification programs (CIPs), which must also be incorporated into banks' BSA/AML compliance programs. However, the minimum standards required in Section 326 are based on the collection of Social Security numbers and driver licenses that contain nothing to prevent the information from being used by others.

Today more than 40 million Social Security numbers (SSNs) are used by two or more people. Valid driver licenses and passports are fraudulently obtained on a daily basis by individuals presenting falsified and stolen birth certificates. Personal information (including the data contained in the databases of information aggregators such as LexisNexis and Kroll and credit reporting agencies Equifax and Experian) is sold on the internet for pennies thanks to computer compromises and data crimes. Yet information and documents are the primary means by which consumers are currently verified for banking and payment services today.

Current customer screening methods have led to the existence of millions of duplicate, alias and synthetic identities. The technology, crimes and criminals are highly sophisticated and the exploitation has heightened to previously unimaginable levels.

As we move into a digital environment in which new customers are increasingly on-boarded through remote channels, new account screening processes are based on software that is driven by the aggregation and analyses of personal information. Identity is verified through a broken system that matches biographic data submitted by an individual to the biographics stored by the companies that compile, aggregate and resell information as a service.

Now the attributes used for identity (especially by innovative payment networks) have been expanded to include such things as email addresses and cell phone numbers, which are even more readily available and easily manipulated than date of birth or SSN.

These broken, biographics-only approaches are regressive solutions that have driven the loss of privacy and are costly, time consuming and easily exploited by fraudsters. The outcome is verified information, not verified identities.

Database vulnerabilities and breaches will continue because the biographics stored within consumer databases are the key to establishing an identity, hiding criminal activity and committing fraud. The threat of data compromises will not diminish until the information held within these databases is no longer of value to hackers and those seeking to exploit it.

The National Institute of Standards and Technology (NIST), the federal technology agency that works with industry to develop and apply standards in technology and innovation, does not accept biographics for identity. NIST defines identity as "the set of physical characteristics by which an individual is uniquely recognizable," and identification as "the process of discovering the true identity of a person from the entire collection of similar persons." Yet the developers of identity systems and information resellers continue to promote biographics for identity; and the verification of biographics for the process of identification.

The lack of a unique customer identification standard is what will undermine the future of payments.

THE SOLUTION – STANDARDIZED UNIQUE IDENTIFICATION PROCESS

The solid foundation for an efficient, safe and accessible payment system is the implementation of a **standardized unique identification process**. This process must ensure that a living human being is attached to each account; and that a multi-sector third party has confirmed the uniqueness of the consumer identity outside the walls of any single organization.

The result is the issuance of a new customer identifier that is linked to the customer, belongs to the customer and is not duplicated within any organization. This truly unique identifier links each customer to only one identity, regardless of payment network or institution used, thus preventing the existence of multiple, duplicate and synthetic identities within and across institutions and payment networks. Within institutions and networks, the identifier enables correct, consistent and comprehensive linking across accounts and lines of business and facilitates variations in biographic data, such as the intermittent use of middle initials or nicknames. The customer's identifying characteristics enable real-time verification at subsequent identity critical interactions.

WHAT THIS SOLUTION PROVIDES

A standardized unique identification process **isolates user identity and proactively implements a critical step to weeding out synthetics and criminal activity in the U.S. payments system**. It is essential to preserving the integrity of the payments system and enabling the innovations that will lead to the desired outcomes envisioned by the Federal Reserve Banks. The proposed process is also accessible to any network and virtually all end users. This enables efficiencies that are otherwise impossible without compromising safety and security.

A unique identification standard is the opportunity to implement a solution for customer identification, identity verification and account matching that is not dependent on the use of the SSN, lessening the vulnerability to banks from the reliance on SSNs that can be falsely aligned and fraudulently used.

This proactive approach is a way to protect payment services, end users and financial institutions from financial crimes, fraud losses, regulatory action and reputational harm. It is the most appropriate and effective response to the challenging situation outlined.

Finally, the new identifier will bring integrity to the end-to-end payment process and enable convenient, cost effective and timely cross border payments. This is accomplished by uniquely identifying users at both the point of payment origination and at receipt; and utilizing the identifier to streamline the payments process, including notification and reconciliation. The unique customer identifier **allows account details to be masked and will serve as the needed tool** to achieve many of the improvements that will lead to the desired outcomes envisioned by the Federal Reserve Banks.

INCONSISTENCY EQUATES TO VULNERABILITY

While new electronic networks are bringing alternatives to consumers, they are evolving without uniformity and consistency, especially regarding the processes following for account opening and customer due diligence. Many thought leaders note concern in this lack of uniformity and consistency, and their fear is justified. Inconsistency equates to vulnerability.

Following 9/11, the federal government – after discovering that inconsistencies in the issuance processes for identity credentials enabled the terrorists to accomplish their tasks – set standards for the identification of government employees in order to safeguard networks and our country's infrastructure from terrorists and those linked to terrorist organizations. This standard, known as Homeland Security Presidential Directive or HSPD-12, requires the capture of physical characteristics – finger and facial images – during an initial identification process to ensure that the individual has not fraudulently obtained a secure credential using a multiple identity.

Building a payments system with a standard for unique identification will start the process to secure our nation's financial infrastructure from money laundering, terrorist financing and financial crimes. This standard must be applied to all participants, regardless of size. If not, the weakest link will undermine the entire system. Uniformity and consistency are not a desired outcome, they are a necessary one.

Therefore, it is imperative that the Federal Reserve Banks work with industry to create processes and tools that are inclusive of all entities that move money, whether a traditional institution or a new entrant.

The Federal Reserve Banks can most effectively drive payment system improvement forward by creating a viable, workable solution that allows for the evolution of two tiers of payment services. These two tiers will accommodate both the legacy systems that offer near-ubiquity (and the security, stability and efficiencies that this affords) and the new payment services that are pursuing less stable and therefore less secure processes, while embracing the innovation that will lead to the next-generation payment system.

With leadership from the Federal Reserve Banks and participation by stakeholders, the first tier will work to achieve the efficiencies and preferences of end users while developing increased security and privacy.

Payment networks that seek to avoid standards and fail to apply the fundamental steps that will safeguard the payment system will move to the second tier. These services, while providing short-term options for a digitally-focused group of consumers, will, in the end, become the networks sought out for nefarious activity. Eventually consumers seeking greater security will move to the first tier and fraudsters will move to the other, placing networks that fail to align with standards at risk of criminal behavior, which will lead to losses to fraud and reputational harm, increased scrutiny, and regulatory action and enforcement.

Thank you again for the opportunity to comment. I would be happy to discuss this in more detail and work with the Federal Reserve Banks and any appropriate committees moving forward.

Sincerely,

Larry Aubol

Larry Aubol, CEO