Statement of

Mark Nelsen

Senior Vice President, Risk Products and Business Intelligence

Visa Inc.

House Ways & Means Subcommittee

on

Oversight

Hearing on

The Use of Data to Stop Medicare Fraud

March 24, 2015

Chairman Roskam, Ranking Member Lewis and Members of the Subcommittee, my name is Mark Nelsen and I am Senior Vice President, Risk Products and Business Intelligence with Visa Inc. Thank you for the invitation to appear before the Ways & Means Subcommittee on Oversight to discuss some of the ways Visa uses predictive analytics and data insights to help prevent fraud. I hope my testimony will provide members valuable perspective as the Subcommittee examines ways to help reduce Medicare fraud. While I am not an expert in healthcare or here to speak to the specifics of Medicare fraud, I did want to share what Visa does in the payments industry to combat fraud as our experience and perspective might be useful to the Subcommittee.

For more than 50 years, Visa has enabled consumers, businesses and governments to make and receive payments across the globe. As a global payments technology company, we connect financial institutions, merchants and governments around the world with credit, debit and prepaid products. Visa works behind the scenes to enable hundreds of millions of daily transactions, powered by our core processing network – VisaNet. Visa invests heavily in advance fraud-fighting technologies to help make digital commerce more convenient, reliable and secure.

As a leader in security, we recognize that there is no silver bullet solution to protecting against fraud. There are many different payment environments and types of fraud. A layered approach that includes a combination of technology, processes and people is required to prevent fraud, and the use of data analytics is a critical component in making all three of these areas effective.

Last year alone, we processed more than 66 billion transactions in global commerce across more than 200 countries. Since the 1990s, Visa payment volume has increased more than one thousand percent, while the rate of fraud actually declined by two-thirds over the same time period.

One of the core tools Visa uses to help limit fraud and make commerce more secure is predictive analytics to identify suspicious transactions before fraud can happen. Our use of data, modeling and analytics help us keep our fraud rates low and stable at less than six hundredths of a percent – that's six cents for every hundred dollars transacted.

Predictive Analytics

Visa's analytics are among the most advanced in the payments industry and have helped to identify and prevent billions of dollars of fraud. We evaluate up to 500 unique data elements to spot suspicious transactions as they are occurring, making it more difficult for criminals to use stolen information. We've invested in developing processes and analyzing the data we have to differentiate the good transaction behavior from the bad. This allows us to identify patterns across the payments industry to help predict potentially fraudulent behavior before a transaction is completed. A key aspect in identifying these patterns is the continuous feedback loop we have built to ensure that financial institutions are able to inform Visa in the event that fraud does occur.

Visa Advanced Authorization is the foundation of our analytics capabilities and provides an instantaneous rating of a transaction's potential for fraud by examining such factors as transaction history, geo-location, transaction velocity, recent fraud and other relevant information. This rating occurs as part of the transaction authorization process and enables the issuer to make a more informed decision about whether to accept or decline the transaction, right at the point of sale. As Visa has visibility across our global network with thousands of issuers, we can use this valuable information to help detect potential fraud. All of this happens today, in the background of every single transaction that Visa processes, in less than a millisecond.

Visa is also beginning to provide this same type of intelligence to merchants. A recent pilot with Chevron resulted in a 23% reduction in the rate of fraudulent transactions at automated fuel pumps. The service is now live at more than 25,000 gas stations nationwide. We believe that providing intelligence to our key stakeholders enables everyone to improve their stewardship of trust in the payments ecosystem. This new initiative highlights the value that analytics can provide to address an area where we have seen a higher propensity for fraudulent activity.

Common Point of Purchase Detection

Another key element of security and fraud prevention that we apply is a method called “Common Point of Purchase” or “CPP.” Card issuing banks and payment networks use advanced analytical tools to search millions of transactions in order to identify those unique locations that show a pattern of genuine transactions followed by suspicious activity on the same card. Such a pattern can indicate a data breach. As with Visa Advanced Authorization, we look at historic data to build a picture of what’s normal for merchants and the individual accounts used at each location. What is the typical daily spend amount? What is the typical approve/decline rate? What is the average ticket size? What is the average cross-border spend? We then compare that picture to what is happening now, and look for deviations. The deviations become signals that lead to the source of a potential data compromise and allow us to further improve our predictive analytics to prevent future fraud.

Criminals know we're searching for patterns, so we are constantly working to improve our analytics. We incorporate new sources of data as they become available, such as device identification and geo-location, and we are constantly working to enhance our modeling techniques to yield the best possible results. As criminal attack vectors evolve, we too follow suit and continue to improve, refine, and advance our fraud fighting solutions through significant investment, innovation and constant vigilance.

In closing, the reality is that criminals, whether they are cyber, healthcare or other fraudsters, will always exist and their tactics will continue to evolve to try to game the system. But the good news is there are sophisticated tools we are developing and evolving to manage these threats. At Visa, we are able to view transactions across the entire ecosystem and use this information to constantly refine our analytics. More data means that we can more quickly identify trends and work to find new ways to sharpen the analytics to identify trends more quickly. We have a centralized processing system and a strong feedback loop from our stakeholders. This allows us to monitor and respond quickly. Of course, technology cannot completely eliminate human error or internal threats, so it remains critical for businesses to adopt strong policies that are effectively implemented by their employees. Criminals are a common foe and each sector must work together to protect against their respective challenges.

Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.