Fair Isaac Corporation
3661 Valley Centre Drive
San Diego, CA 92130 USA
T 858 369 8000
F 858 369 8001
www.fico.com

Make every decision count.™

September 9, 2016

Ms. Nakia Grayson
National Institute of Standards of Technology
101 Bureau Drive, Stop 200
Gaithersburg, MD 20899
Submitted at *cybercommission@nist.gov*

RE: Input to the Commission on Enhancing National Cybersecurity

Dear Ms. Grayson:

Fair Isaac Corporation, FICO, appreciates the opportunity to provide comments in response to the notice and request for information published in the Federal Register, Vol. 81, No. 154, on August 10, 2016, by the National Institute of Standards and Technology (NIST) regarding current and future states of cybersecurity in the digital economy. Executive Order 13718 charged the Commission on Enhancing National Cybersecurity with making recommendations to strengthen cybersecurity, develop new technical solutions, and bolster cybersecurity partnerships among federal, state and local governments and the private sector.

FICO'S EXPERIENCE AND EXPERTISE

FICO is a Silicon Valley-based analytics and decision management software company. For many years, the FICO® Score has been the gold standard in the financial services industry for credit risk underwriting. In addition, the FICO® Falcon® Fraud Manager software and related streaming artificial intelligence models have comprised the world's leading payment card fraud protection solution. Recently, FICO has turned its attention to cybersecurity analytics.

In April 2016, FICO announced it had partnered with iboss Cybersecurity to embed FICO's artificial intelligence based cyber analytics as part of the iboss node-based, direct-to-cloud, containerized platform, a leading solution for cybersecurity and malware protection. Since then FICO announced that is developing a FICO® Enterprise Security Score, which will rank an organization's level of cybersecurity risk. The score utilizes predictive analytics to forecast the likelihood of a material data breach over the subsequent 12-month period. This solution will complement FICO's analytics for threat detection and will be an easy-to-understand metric that will facilitate board-level risk assessment, third-party vendor management, and cyber breach insurance underwriting. To further this effort, in June 2016 FICO acquired QuadMetrics, an innovative cyber risk security scoring company based in Ann Arbor, Michigan.

CRITICAL INFRASTRUCTURE CYBERSECURITY

Protecting the nation's critical infrastructure through cybersecurity awareness and innovation must be considered a top priority for this and future administrations. FICO believes that technological advances, in the form of advanced analytics, provide great promise in protecting our nation's most important assets. However, there are significant challenges ahead.

- ***Shortage of Trained Resources***. The volume and complexity of networks and data continues to grow, moving beyond expert capabilities. There is a shortage of trained resources in the field of cybersecurity to confront the increasing demand of cyber threats. This resource problem extends beyond just training more cybersecurity professionals; it also requires highly skilled personnel to keep pace with the rapidly evolving cyber environment, where new threats are introduced each day and demand quick identification of vulnerabilities.

- ***Many threat detection approaches are ineffective***. The majority of technology being utilized to detect cyber threats is not intelligent enough. Many organizations are utilizing rules-based or signature based detection, which do not quickly adjust to changing cyber technology and conditions. This often leads to a huge volume of alerts, and a high percentage of false-positives, which cannot be efficiently prioritized, reviewed and accurately assessed.

- ***The time between a cyber-attack and its recognition is too slow.*** Perhaps the most critical factor in stopping attacks is time. Approaches that depend on the definition and codification of an attack signature create a considerable detection lag and typically require the attack to be successful before recognized and codified.

Behavioral Analytics. In protecting our nation's critical infrastructure, organizations need to invest in behavioral analytics to replace the primary solutions found in the market today; those that are signature-based and generate a plethora of alerts cannot be efficiently monitored or managed. Investing in behavioral analytics will also address the other primary weakness of these solutions, which is the long time to resolution, or no resolution and lingering/ongoing threats. The best way to effectively combat cyber threats is to learn from best practices and success from other business problems with similar high volume data and abnormal user and entity identification needs. From those experiences, the solution is to leverage an advanced analytics approach that operates in real-time, prioritizes alerts and uses self-learning analytics to determine new unknown attacks as they happen. Given the volumes of data involved, the scale of attacks that are occurring and the complexity of identifying signals of anomalous behavior, only self-adapting analytic models based on machine-learning algorithms will be effective.

Real-time streaming analytics. FICO believes the market must adopt real-time streaming analytics that utilize machine learning to immediately detect and flag anomalous activity. We have seen the benefits derived from advanced analytics which target emerging threats with layered analytics that are not limited to heuristics or peer group comparisons. These self-learning, user and entity behavior analytics (UEBA) adapt continuously to reduce false positives. Furthermore, this capability provides intelligent risk ranking/probability from 1-999 on entities like devices and users. To address both a lack of resources and the absence of a cutting-edge knowledge base, the information identified by the analytics needs to be presented in a form that is simple to understand, such as an alert risk ranking, with associated reason codes to point the security analyst to the source of the risk concern. This will ensure that the analyst directs his attention to addressing immediate threats while not wasting time on less urgent or lower level concerns. This is essential for operationalizing cyber security threat detection analytics.

Power of the cloud. Cloud computing will continue to play a critical role in combatting cyber threats. Cloud solutions can be deployed and managed by a professional team that resides outside an organization's premises limiting the IT resources and support needed to implement cyber solutions. In addition, the cloud is making cybersecurity more accessible to all sizes of organizations, extending beyond critical infrastructure. The benefits derived are significant as cyber criminals target organizations that they perceive do not have the in-house resources to address cyber vulnerabilities.

The consortium approach. We believe that a cybersecurity ecosystem needs to be bolstered with greater collaboration among similarly situated companies. This is not a problem that each company or organization should have to fight alone. We suggest a model similar to the one that FICO introduced in the 1990s to combat credit card fraud. Thousands of firms that use the FICO Falcon Platform contribute data from billions of transactions to a data consortium, which enables FICO analytic scientists to build more powerful artificial intelligence models for specific regions and payment products. These models are, of course, more powerful than models developed from any individual firm's experience, as they are more sensitive to newly derived patterns of attack across all the contributors' data. In just a few years, after the introduction of FICO Falcon Fraud Manager in 1992, credit card fraud in the U.S. was reduced from 18 basis points of card sales to six, and has been held at or around this level ever since.

In the cybersecurity arena, FICO supports the ongoing work of Information Sharing and Analysis Centers (ISACs) as well as efforts by the federal government to promote information sharing between the public and private sectors. In addition, we believe that the development of a cybersecurity consortium where clients share user behavior data to feed and inform real-time analytics can provide valuable enhancements to the tools being used to combat cyber threats. Such data sharing arrangements can inform and improve analytic models by giving analysts the ability to react to changing threat landscapes and contributors' real-time experiences. We refer to this as 'actionable data sharing'. This approach also has the advantage of crowd-sourcing the

best analysts' feedback into a central repository for the purpose of updating an analytic model that benefits all. In fact, FICO has recently launched such a consortium through clients using the FICO Cyber Threat Score in the iboss solution.

ENTERPRISE CYBERSECURITY SCORES

Enterprise Cybersecurity scoring is in the very early stages of commercial adoption, but it holds great promise for enterprises to perform their own internal initial risk assessments and monitor progress against an empirically derived score for the enterprise. These scores are designed to provide a benchmark for assessing an organization's security posture. Generally, these scoring algorithms include an external surveillance of an organization's security practices such as open ports, vulnerabilities, and expired certificates, as well as publicly available intelligence, which may include open source malware intelligence and hacker/dark web chatter.

Most commercial offerings today offer point-in-time analysis of an organization's network security based primarily on judgmental scoring – simply adding or subtracting points based on risk factors present during a snapshot in time. We believe that an empirical approach is a more trustworthy method. This approach would analyze as much data as possible, and would calculate the likelihood of an organization suffering a significant material breach event during the next 12 months. This alone will place cybersecurity scoring on the same level as other underwriting methodologies, which explicitly tie data elements and derived features of cyber security risk to predicted breaches.

Security scoring can also enhance risk analysis when used to perform due diligence on partners and vendors. This is a critical need to help organizations in industries like financial services, where regulatory guidance has been issued and supervisory exams have emphasized the importance of a strong vendor management program. To date, the cybersecurity industry has lacked a consistent method of measuring and communicating the cyber risks associated with enterprise security. As a result, Chief Information Security Officers and executive teams struggle to measure the results of their efforts. IT leaders also struggle with finding ways to measure and manage the long-term risk of data loss. With the introduction of Enterprise Security Scores, FICO provides an independent, external risk assessment that allows cybersecurity to be managed in ways that parallel other forms of risk management. In this respect, the FICO Score, the standard in assessing credit risk for decades, is a good comparison, as it has provided a single metric that is used by lenders, mortgage brokers, regulators, and consumers to understand consumer credit risk. It has also facilitated the efficient and transparent securitization of debt. We expect the FICO Enterprise Security Score to have similarly profound impacts in cybersecurity.

CYBERSECURITY INSURANCE

Cybersecurity scoring may also be a tool for the cyber insurance industry. The increased use of organizational security scores can provide insurers with increased risk assessment precision while also providing insights for organizations to improve their own security, resulting in lower insurance premiums and greater protections for the general public. In insurance underwriting, as in credit risk assessment, increased predictive power leads to lower costs for most customers, as it increases the ability of insurers to differentiate good from bad risks. Without this information, more good and bad accounts are lumped in together, and the price those accounts pay reflect this lack of risk differentiation.

Data breach insurance is now considered a necessity for large organizations. Premiums are expected to grow in the next decade from $2B today to $20B by 2025 (20% CAGR). Despite this dramatic growth, the risk assessment and ratemaking processes employed by these insurers are immature and often proprietary. There is no accessible claims database that could assist insurers in risk analysis and rating, and promote a more consistent experience for other organizations and their customers.

In addition, smaller, less sophisticated organizations may be unaware of the potentially devastating consequences of a data breach for their organizations and their customers. Moreover, the cost of cybersecurity insurance, which will necessarily include a risk premium to protect insurers who are unsure of the risk being assumed, will be a deterrent to smaller organizations. It may be necessary to have a national reinsurance program (like flood insurance) or mandated state programs (like auto insurance or earthquake insurance) to ensure that business are correctly protecting customer data and actively working to remediate weaknesses that can be exploited by cyber criminals.

CYBERSECURITY RESEARCH AND DEVELOPMENT

Government-funded research remains vitally important to the development of new techniques and solutions to combat cybersecurity threats. FICO has first-hand experience of the value of cybersecurity innovation that has occurred through both private and public funding channels. The technology obtained by FICO in its QuadMetrics acquisition was developed at the University of Michigan through funding by the Department of Homeland Security. FICO has been able to enhance Quadmetrics's core intellectual property with patented analytical techniques. We believe research in this field supported by government funding must continue in order to ensure that cybersecurity innovation in the U.S. reaches its full potential, and the U.S. does not fall behind other nations. FICO endorses and encourages a strong emphasis on artificial intelligence and deep learning in the cybersecurity space.

Thank you again for this opportunity to comment on the Commission's request for information. Should you have any questions, please feel free to contact me.

Sincerely,

Scott Zoldi
Chief Analytics Officer
FICO
scottzoldi@fico.com