NYS
SOCIETY OF
CPAs
NYSSCPA

November 11, 2016

Via Electronic Submission

Ms. Cassandra Lentchner
New York State Department of Financial Services
One State Street
New York, NY 10004

By e-mail: CyberRegComments@dfs.ny.gov

Re: Proposed New York Codes, Rules and Regulations—
Title 23. Department of Financial Services—Chapter I. Regulations of the Superintendent of
Financial Services—Part 500. Cybersecurity Requirements for Financial Services Companies

Notice of Proposed Rulemaking I.D. No. DFS-39-16-00008-P

Dear Ms. Lentchner:

The New York State Society of Certified Public Accountants (NYSSCPA), representing more than 26,000 CPAs in public practice, business, government and education, welcomes the opportunity to comment on the above-captioned proposed regulations.

The NYSSCPA's Technology Assurance Committee and Banking Committee deliberated the proposed regulations and prepared the attached comments. If you would like additional discussion with us, please contact Matthew Clohessy, Chair of the Technology Assurance Committee, at (716) 851-8356, Jo Ann Golden, Chair of the Banking Committee, at 315-794-9056 or Ernest J. Markezin, NYSSCPA staff, at (212) 719-8303.

Sincerely,

F. Michael Zovistoski

F. Michael Zovistoski
President

Attachment

NEW YORK STATE SOCIETY OF
CERTIFIED PUBLIC ACCOUNTANTS

COMMENTS ON

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

PROPOSED NEW YORK CODES, RULES AND REGULATIONS— TITLE 23. DEPARTMENT OF FINANCIAL SERVICES—CHAPTER I. REGULATIONS OF THE SUPERINTENDENT OF FINANCIAL SERVICES—PART 500. CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICE COMPANIES

Notice of Proposed Rulemaking I.D. No. DFS-39-16-00008-P

November 11, 2016

Principal Drafters

Matthew T. Clohessy
Jo Ann Golden
Joel Lanz
Yigal Rechtman

NYSSCPA 2016–2017 Board of Directors

F. Michael Zovistoski, *President*
Harold L. Deiters III, *President-elect*
John J. Lauchert, *Secretary/Treasurer*
Gregory J. Altman, *Vice President*
Susan M. Barossi, *Vice President*
Anthony S. Chan, *Vice President*
John S. Shillingsford, *Vice President*
Joanne S. Barry, *ex officio*
Edward L. Arcara
Sol S. Basilyan
Paul E. Becht
Christopher G. Cahill
Jack M. Carr
Salvatore A. Collemi
Mitchell A. Davis
Edward F. Esposito
Joseph M. Falbo, Jr.
Rosemarie A. Giovinazzo-Barnickel
Elizabeth A. Haynie
Elliot L. Hendler
Jan C. Herringer
Patricia A. Johnson
Jean G. Joseph
Barbara A. Marino
Kevin Matz
Mitchell J. Mertz
Jacqueline E. Miller
Tracey J. Niemotko
Kevin P. O’Leary
Iralma Pozo
Renee Rampulla
Brian M. Reese
M. Jacob Renick
Warren Ruppel
Steven A. Stanek
Denise M. Stefano
Janeen F. Sutryk
Michael M. Todres
David G. Young

NYSSCPA 2016–2017 Accounting and Auditing Oversight Committee

Robert M. Rollmann, *Chair*
Charles Abraham
Matthew T. Clohessy
Salvatore A. Collemi
Michael J. Corkery
Lourdes Eyer
Craig T. Goodman
Jan C. Herringer
Adam S. Lilling
Renee Mikalopas-Cassidy
Rita M. Piazza
William M. Stocker III

NYSSCPA 2016–2017 Industry Oversight Committee

Jason I. Barocas, *Chair*
Jeffrey Abramczyk
Anthony Cassella
David P. Dukoff
Alan D. Fishman
Peter H. Frank
Abraham E. Haspel
Natalie Kotlyar
Sean D. Matthews
Madelyn R. Miller
Grant Rapaport
Leonardo Sabino
Jaime L. Scott
Akshay T. Shrimanker

NYSSCPA 2016–2017 Technology Assurance Committee

Matthew T. Clohessy, *Chair*
Moises A. Brito, *Vice Chair*
Faisal Ali
Jeff Behling
Harvey G. Beringer
Michael Carroll
Xin Chen
Jill Johnson
Dekedrian Johnson
Lucas Kowal
Jim Krantz
Joel Lanz
Mikhail Lezhnev
Michael Melcer
Jason M. Palmer
Andrew Phillips
Karina Pinch
Michael Pinch
Michael A. Pinna
Yigal Rechtman
Clayton L. Smith

Robert A. Cohen
David O. Daniels
James C. Goldstein
Heather Heale
Shelly E. Mitchell
John Nasky
Yossef Newman
Joseph B. O'Donnell
Thomas J. Sonde
Cheick Ahmed T. Souare
Rebecca Stockslader
Jonathan D. Willcox

NYSSCPA 2016–2017 Banking Committee

Jo Ann Golden, *Chair*
Ashish Ahlowalia
Joseph P. Athy
Christopher G. Cahill
Catherine Califano
Rekha Chatterjee
John C. Chen
Brian M. Conboy
Sharon Sabba Fierstein
Sai M. Gadwale
Howard M. Gluckman
Jeremy Goss
Wendy R. Grant Mungroo
Andrew J. Greiner
Christopher Halstead
Elias H. Lambros
Hee Woon Lee
Nigyar Mamedova
Matthew McNeill
Edward J. Mueller
Gina Omolon
William Perri
Lorenzo Prestigiacomo
Joseph G. Schiavo
William F. Schwenk
Paul C. Sinaly
Franco Strangis
Allan Tepper
Tammy W. Tien
Katherine M. Tornarites
Daniel J. White

NYSSCPA Staff

Keith Lazarus

New York State Society of Certified Public Accountants

Comments on

Proposed New York Codes, Rules and Regulations—
Title 23. Department of Financial Services—Chapter I. Regulations of the Superintendent of
Financial Services—Part 500. Cybersecurity Requirements for Financial Services Companies

Notice of Proposed Rulemaking I.D. No. DFS-39-16-00008-P

General Comments:

Overall, we support the New York State Department of Financial Services' (DFS) promotion of establishing, enhancing and maintaining robust cybersecurity risk management practices. We agree with the NYSDFS' assessment over the criticality of cybersecurity programs. While we support the objectives of the proposed regulation, we have concerns that it may result in unintended consequences and therefore have general and specific comments aimed to provide greater clarity over the DFS' expected requirements and recommended revisions to better allow impacted organizations to meet the DFS's expectations especially as they relate to management or board certification with compliance with the rule. Our comments pertain to the impacts to banking Covered Entities.

Many financial services companies currently comply with federal and state regulatory requirements such as the Gramm-Leach Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA). Many impacted organizations have already invested in relevant risk management strategies as identified by the Federal Financial Institutions Examination Council ("FFIEC") IT Examination Handbooks and frameworks established by the National Institute of Standards & Technology (NIST), including the Cybersecurity Framework.

While most of the risk management and control objectives of the proposed regulation conceptually aligns with the existing regulatory requirements and best practice guidance, there are specific areas where the proposed legislation differs with or is inconsistent with the above practices. Inconsistent requirements may result in organizations devoting more and in some cases unneeded resources to the administration of cybersecurity practices rather than protecting organization and consumer assets. It would therefore be helpful, as is done with other cybersecurity standards, to have a "cross-walk reference" to allow interested parties to see how the proposed requirements align with existing frameworks and provide more specificity to requirements. (For example, this "cross-walk" is currently provided for the NIST's Cybersecurity Framework and the Center for Internet Security's Top Twenty Controls – two very recognized frameworks amongst the cybersecurity and audit communities.)

In our first general comment, we recommend that the DFS provide guiding principles as to whether financial institutions utilizing effectively designed and operating cybersecurity risk management practices that align with the existing best practice or regulatory guidance (e.g., FFIEC IT Examination Handbooks) could satisfy compliance with the DFS' proposed regulation. This would also include specifying which risk assessment methodologies will be acceptable to the DFS and the nature of evidence with the proposed regulation to be maintained to demonstrate compliance with the regulation; for example, what type of evidence should the certifier be reviewing prior to signing the certification.

Our second general observation of the proposed legislation is that it cites specific controls as examples or explicitly requires the use of specific controls to achieve the risk management objectives of the legislation. Given the pace of change in technology, the inclusion of specific technology control requirements may result in influencing or requiring companies to establish ineffective or outdated controls.

We further recommend annexing prescriptive control design requirements and specific control examples to explanatory supplemental guidance appended to the regulation.

These general comments are expanded upon within the relevant areas of the specific comments section below.

Specific Comments:

Section 500.1(c) Definition of Covered Entity

> *Covered Entity means any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law or the financial services law.*

The term "Covered Entity" is also defined by the Health Information Portability and Accountability Act of 1996 (HIPPA), as amended. We recommend that the DFS consider expanding or modifying their terminology to indicate that a "Covered Entity" under 23 NYCRR 500 is "NYSDFS Covered Entity." By doing so, should references be made to compliance requirements for a "Covered Entity," there will be a differentiation between existing requirements for Covered Entities under HIPAA and the requirements for Covered Entities as defined under the DFS' proposed legislation.

Section 500.1(e) Definition of Information System

> *Information System means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.*

We recommend that the term "information system" be revised more succinctly and defined as "a set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system."

Defining an Information System as a 'discrete set' is duplicative in nature as a 'set' is defined as a discrete collection elements or members. Further, the discussion of what constitutes a "specialized system such as industrial/process controls systems, etc." is too narrowly defined and we recommend the statement end with the term "specialized system."

Section 500.1(f)(2) Definition of Multi-Factor Authentication

> *Multi-Factor Authentication means authentication through verification of at least two of the following types of authentication factors:*
>
> *(1) Knowledge factors, such as a password; or*
>
> *(2) Possession factors, such as a token or text message on a mobile phone; or*
>
> *(3) Inherence factors, such as a biometric characteristic.*

The definition of the "possession factor" component to Multi-Factor Authentication is inconsistent with the definition provided by the FFIEC.[1] Mobile phone text messages are considered by existing regulatory practices as an "Out-of-Band" authentication control and not a "possession factor" element of Multi-Factor Authentication.

We support the use of Out-of-Band Authentication controls as a component to a layered security approach; however, the inconsistencies in defining what constitutes a "possession factor" may cause unintended consequences in a Covered Entity's ability to satisfactorily evidence adherence to the requirements of Section 500.12 (Multi-Factor Authentication) as well as the requirements established by Federal banking regulators.

We recommend that the DFS remove mobile phone text messages from its definition of the "possession factor" component to Multi-Factor Authentication and create a separate definition for Out-of-Band Authentication such that the DFS' definition of authentication control terminology is consistent with existing regulatory guidelines followed by financial institutions.

Further commentary on the use of Out-of-Band Authentication is expanded upon in our comments to the requirements of Section 500.12.

Section 500.1(g)(3) Definition of Nonpublic Information

> *Nonpublic Information shall mean all electronic information that is not Publicly Available Information and is:…*
>
> *…(3) Any information, except age or gender, that is created by, derived or obtained from a health care provider or an individual and that relates to the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family or household, or from the provision of health care to any individual, or from payment for the provision of health care to any individual;*

We recommend that the DFS remove the exclusion of age and gender from the definition of non-public information as it conflicts with the definition set forth in Section 500.01(g)(4) which states that "any information that can be used to distinguish or trace an individual's identity."

Age and gender are distinguishing pieces of information for an individual's identity, especially in the context of cross-channel fraud, which may incorporate interaction with telephone banking customer service centers or physical retail branch into a fraud scheme, whereby mismatches to

[1] FFIEC, *Authentication in an Internet Banking Environment* (October 2005)

an individual's gender or general age can serve as red flags in identifying potential cases of identity theft.

Further, age is a relative term based on an 'as of' date. Accordingly, an explicit exclusion of age could lead to the misinterpretation that dates of birth, the data point to determine age, is also excluded. Dates of birth are commonly utilized as one piece of authenticating information for telephone banking customer service centers.

> Section 500.1(k) Definition of Risk-Based Authentication
>
> *Risk-Based Authentication means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.*

Current FFIEC guidance[2] on the subject recommends a layered security approach which has several options available to establishing a well-controlled cybersecurity environment. The discussion on Risk-Based Authentication is appropriate, however, we recommend removing "challenge questions" as a specific example within the definition as it may lead to misinformed interpretations that the use of challenge questions would solely be considered an effective control or that their use is a specific requirement.

The use of challenge questions is likely to continue to evolve over time. Challenge question controls can be defeated by data aggregation tools and social media data if commonly used questions or social media searchable questions are utilized. As such, use of challenge questions are best utilized when they are *one* component of a risk-based layered security approach.

> Section 500.2(a) Cyber Security Program
>
> *Cybersecurity Program. Each Covered Entity shall establish and maintain a cybersecurity program designed to ensure the confidentiality, integrity and availability of the Covered Entity's Information Systems.*

We agree with the proposed regulation, but recommend that the reference of a cybersecurity program should indicate that the design, implementation, monitoring, and activity within such a program should be *documented*. We recommend that the documented program should contain sufficient detail that would enable "an experienced auditor or regulator to understand the thought process, risk assessment, findings, and conclusions of the NYSDFS Covered Entity."

> Section 500.3(a) Cybersecurity Policy
>
> *Cybersecurity Policy. Each Covered Entity shall implement and maintain a written cybersecurity policy setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall address, at a minimum, the following areas…:*

[2] FFIEC, *Supplement to Authentication in an Internet Banking Environment* (June 2011)

We agree with the regulation's requirement to establish a cybersecurity policy, but are concerned that while the requirement outlines the objectives that should be addressed within the cybersecurity policy, the regulation does not provide sufficient granularity to effectively assess compliance with the DFS' expectations of the content that should be incorporated into the policy.

We recommend the DFS provide further guidance on whether there are specific requirements or comparable benchmarks (e.g., FFIEC IT Examination Handbook or NIST guidelines) that should be consulted for further information and expectations as to the functional content and considerations that should be incorporated within the cybersecurity policy.

> Section 500.04(a) Chief Information Security Officer
>
> *Chief Information Security Officer. Each Covered Entity shall designate a qualified individual to serve as the Covered Entity's Chief Information Security Officer (CISO) responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy.*

We agree with the regulation to designate a CISO, but recommend the DFS provides further specificity to what the DFS' expectations are in determining whether someone is a 'qualified individual.'

> Section 500.04(b) Chief Information Security Officer Report
>
> *Report. The CISO of each Covered Entity shall develop a report, at least bi-annually, as described herein…*

We agree with the requirement to establish reporting processes and have requests for clarifying components of this section:

We recommend the DFS replace the term "bi-annually" with semiannually in order to eliminate the ambiguity over which definition of the term bi-annually is intended for this requirement — two times per year or once every two years.

We recommend the DFS provide further specificity to DFS' expectations on what basis the CISO's assessments in the bi-annual report is expected to be based upon; such as the results of management assessments and reviews; internal and external audit activity related to information security; third-party reviews of the information security program and information security measures; and other internal or external reviews designed to assess the adequacy of the information security program, processes, policies, and controls.

> Section 500.05(a)(1) Penetration Testing and Vulnerability Assessments
>
> *The cybersecurity program for each Covered Entity shall, at a minimum, include:*
>
> *(1) penetration testing of the Covered Entity's Information Systems at least annually;*

In general, we agree with the requirement to conduct periodic penetration testing of a Covered Entity's Information System; however, there is much disagreement within the profession as to what constitutes a penetration test. In some situations, especially with smaller organizations, an independent security test that identifies the exploit and does not exploit the vulnerability may be sufficient. Also, it is unclear as to whether the penetration test must include social engineering components or be limited to technical vulnerabilities.

We recommend that the DFS clarify its expectations as to what specific standard(s) or methodology should be followed in conducting a penetration test and to what it extent the covered entity can decide on an appropriate scope for testing based on a properly completed risk assessment.

We also recommend that the DFS clarify its expectations as to whether the party conducting the penetration test should be independent of the Chief Information Security Officer's reporting line, such as an Internal IT Audit or an External IT Audit service provider.

Section 500.07 Access Privileges

> *As part of its cybersecurity program, each Covered Entity shall limit access privileges to Information Systems that provide access to Nonpublic Information solely to those individuals who require such access to such systems in order to perform their responsibilities and shall periodically review such access privileges.*

We agree with the requirements to limit access privileges to Nonpublic Information; however, use of the term "individual" could be misleading. Access should be viewed as access to any agent – a natural person, an entity, or a computer program executing inside or outside the system of the Covered Entity.

We recommend that the term "individual" should be replaced by "agent with access", and the term "agent with access" should be broadly defined. This is partially addressed in 500.11 but the terminology for "individual" and "third party" are not cross-referenced.

Section 500.09(a) Risk Assessment

> *At least annually, each Covered Entity shall conduct a risk assessment of the Covered Entity's Information Systems. Such risk assessment shall be carried out in accordance with written policies and procedures and shall be documented in writing.*

We agree with the overall requirement to conduct a risk assessment; however, we recommend that there should be an internal consistency between the vulnerability assessment requirements (Section 500.05) for being at least quarterly and the requirements of this section to conduct a risk assessment at least annually.

Vulnerability assessments are completed in part to inform and quantify risk exposure as a part of a risk assessment process. The timing variances inherent in the regulation would allow for a vulnerability to be identified Q1 of a certain year, but the risk assessment and updates to risk management practices could potentially not be required until Q4 of the same year. This could mean that an identified vulnerability could lapse nine months without mitigation, and would still satisfy the requirements of the regulation.

We recommend that the requirements of 500.05 and 500.09 should be synchronized or clarified such that management establishes risk tolerance levels and if a vulnerability or other information is identified through ongoing monitoring activities that exceed the defined risk tolerance, would require an interim update to the risk assessment outside of a Covered Entity's pre-established periodic review schedule and should occur within a shorter window of time, such as 30 days.

Section 500.12(a)(1)-(3) Multi Factor Authentication

Multi-Factor Authentication. Each Covered Entity shall:

(1) require Multi-Factor Authentication for any individual accessing the Covered Entity's internal systems or data from an external network;

(2) require Multi-Factor Authentication for privileged access to database servers that allow access to Nonpublic Information;

(3) require Risk-Based Authentication in order to access web applications that capture, display or interface with Nonpublic Information; and

We support the use of Multi-Factor Authentication as a component to a risk management practice; however, we have concerns regarding the regulation's absence of also recommending the use of a risk based assessment over authentication practices to determine if additional risk based layered security practices should be employed as well.

Multi-Factor Authentication cannot, singularly prevent cyber-crime, but rather should be viewed as one of several components to a suite of risk management controls that holistically provide an effective control environment.

We are concerned that the proposed legislation's requirement to establish Multi-Factor Authentication without also recommending the use of risk assessments to determine what *additional* practices may be warranted may unintentionally result in Covered Entities implementing control procedures to the letter of the law and solely implementing and relying upon Multi-Factor Authentication for their authentication practices.

We recommend that the regulation require that a risk based process be established and if the risk assessment process results in any other procedures, policies, or controls that could augment the Multi-Factor Authentication paradigm, that these procedures, policies and controls must be added.

Further, pursuant to our commentary in Section 500.1(f) in defining Out-of-Band Authentication, we recommend the DFS supplement its requirements for requiring Multi-Factor Authentication to also allow for Single Factor Authentication when coupled with Out-of-Band Authentication.

Use of either Multi-Factor Authentication or Single Factor Authentication coupled with an Out-of-Band Authentication control will henceforth be referred to as "Enhanced Authentication."

Section 500.12(a)(4) Multi Factor Authentication

Multi-Factor Authentication. Each Covered Entity shall:…

…(4) support Multi-Factor Authentication for any individual accessing web applications that capture, display or interface with Nonpublic Information.

We support the DFS objective to increase the availability of Enhanced Authentication; however, we request that DFS further clarify the requirements to “support” Enhanced Authentication.

Due to the costs associated with issuing physical token devices to achieve the possession factor for Multi-Factor Authentication, retail digital banking customers would commonly achieve Enhanced Authentication through either use of software generated tokens from their mobile device for a “possession factor” to achieve Multi-Factor Authentication or use of a mobile device text message one time use code utilized to achieve an Out-of-Band Authentication.

These approaches are effective in the context of customers accessing a web application from a personal computer that are able to use their mobile device to facilitate Enhanced Authentication, but Covered Entities may have challenges in effectively supporting Enhanced Authentication in the context of users accessing a web application from their mobile device.

The inherent challenges to providing Enhanced Authentication and some forms of layered security for the mobile banking channel are commonly addressed by Covered Entities through the use of a risk-based approach, which may include opting to limit the dollar amount or types of transactions that consumers are able to execute through a mobile channel in order to reduce the inherent risk of the mobile banking channel.

We therefore recommend that DFS clarify whether it is expected that Enhanced Authentication is required to be supported for *all* channels available to individuals or if compliance with the regulation can be met if Enhanced Authentication is supported for at least one channel available to a customer.

We also recommend that DFS clarify what the “support” requirements are for Covered Entities that have customers who do not have the capability to comply with the Covered Entity’s Enhanced Authentication practices, including—but not limited to—the following scenarios:

- If, under an assumption that it is acceptable to support Enhanced Authentication for at least one channel available to a customer, and the Covered Entity has made Enhanced Authentication available through its personal computer web-based access channel, what are the support requirements for customers who only utilize mobile phone based access channels and do not utilize or have access to personal computer access channels?

- If a Covered Entity’s Enhanced Authentication controls relies upon a mobile device for a software generated token code or text message, what if the customer does not own a mobile device, does not own a mobile device that has the capability to support the necessary software to generate token codes, or resides in an area without the requisite cellular tower service needed to be capable of receiving text messages?

We urge DFS to consider the implications of this clarification in the context that Covered Entities, in order to ensure that they are able to comply with this regulation, may be required to terminate or refuse customer access to digital banking services if the Covered Entity cannot support Enhanced Authentication for customers unable to comply with the Covered Entity’s Enhanced Authentication controls and may result in inhibiting certain individual’s access to digital banking services in the State of New York.

Section 500.17(a) Notices to Superintendent

> *Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent of any Cybersecurity Event that has a reasonable likelihood of materially affecting the normal operation of the Covered Entity or that affects Nonpublic Information. The Covered Entity must notify the superintendent as promptly as possible but in no event later than 72 hours after becoming aware of such a Cybersecurity Event.*

We agree with the requirement to provide notification if a breach occurs. We recommend that DFS clarify whether or not it is assumed that a violation of this law is presumed to have occurred if a data breach occurs.

Section 500.17(a) Notices to Superintendent

> *Annually each Covered Entity shall submit to the superintendent a written statement by January 15, in such form set forth as Appendix A, certifying that the Covered Entity is in compliance with the requirements set forth in this Part. Each Covered Entity shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years.*

We agree with the requirement for management to certify compliance with the regulation. We recommend DFS clarify what the culpability of signors of the compliance attestation is.

Section 500.18(a)(1) Limited Exemption

> *(a) Limited Exemption. Each Covered Entity with:*
>
> *(1) fewer than 1,000 customers in each of the last three calendar years*

We agree with the risk-based exemption threshold established by this subpart, however, we do not agree that measuring by "customer" is appropriate in this setting. Covered Entities may have access to and store non-public consumer information of individuals that are not their customer, such as Covered Entities that act in an agency capacity servicing other Covered Entities' customers, Covered Entities that have affiliate relationships with another Covered Entity who has a customer base that opted in for affiliate information sharing and Covered Entities that process applicant information for products or services.

We therefore recommend that the risk based exemption threshold be measured not by the number of customers, but by the number of persons as defined in 500.01(h), whose data is accessible by the Covered Entity.

Additional Considerations

Risk Acceptance Practices

We suggest that DFS adds a section to the regulation that clarifies to what extent a risk acceptance process can be used as a component to evidencing compliance with the law, so long as they adhere to best practice guidance such as the guidelines outlined by the FFIEC's *Information Technology Examination Handbook – Information Security*, issued in September 2016.

Independent Validation

We suggest that DFS incorporate a component that would require the cybersecurity program requirements of this regulation to be subject to a periodic independent risk based audit validation conducted by a qualified independent party to validate the effective design and operating effectiveness of the governance oversight and control environment established by the CISO.

Definition of Customer

We recommend DFS add a definition for the term “customer” in Section 500.01.