Finance & Risk: Examining NYDFS Part 504

Wednesday, 28 February 2018 | 8–9:30 a.m.
Breakfast, 8-8:30 a.m. | Program, 8:30–9:30 a.m.

Fordham Law School
Skadden Conference Center
150 West 62nd Street, New York City

CLE COURSE MATERIALS
<table>
<thead>
<tr>
<th>CONTENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Examine NYDFS Part 504</td>
</tr>
<tr>
<td>2. NYDFS Part 504</td>
</tr>
<tr>
<td>3. NYDFS Regulation 504 Frequently Asked Questions</td>
</tr>
<tr>
<td>4. NYDFS Part 500</td>
</tr>
<tr>
<td>5. NYDFS Regulation 500 Frequently Asked Questions</td>
</tr>
<tr>
<td>6. Criminal Solicitation, 4th Degree</td>
</tr>
<tr>
<td>7. Criminal Solicitation, 5th Degree</td>
</tr>
<tr>
<td>8. Offering a False Instrument for Filing, 1st Degree</td>
</tr>
<tr>
<td>9. Offering a False Instrument for Filing, 2nd Degree</td>
</tr>
<tr>
<td>10. Falsifying Business Records, 1st Degree</td>
</tr>
<tr>
<td>11. Falsifying Business Records, 2nd Degree</td>
</tr>
<tr>
<td>12. Facilitation, 4th Degree</td>
</tr>
<tr>
<td>13. Facilitation, 5th Degree</td>
</tr>
<tr>
<td>14. Facilitation, 6th Degree</td>
</tr>
<tr>
<td>15. Attempt to Commit a Crime</td>
</tr>
<tr>
<td>16. Evolving AML Journey: Balancing Internal, External and Virtual Workforces</td>
</tr>
</tbody>
</table>
EXAMINING NYDFS
PART 504

FORDHAM / ACCENTURE
COMPLIANCE SERIES
FEBRUARY 2018
• Moderator and Panelist Introductions
• Executive Summary
• DFS 504 Compliance Timeline
• Common Challenges for Consideration
• What makes and effective monitoring programme
• Regulation 504 and the NYS Penal Code
• What questions do you have for our panelists?
MODERATOR AND PANELIST INTRODUCTIONS

Alice BrightSky
Fordham
Senior Director, Compliance Programs

As senior director of Fordham Law's compliance programs, Alice BrightSky manages the School's compliance initiatives, including the LL.M., M.S.L., and executive education programs in compliance. She brings more than 10 years of experience in the field, with a focus on developing, implementing, and managing anti-money laundering (AML) and know-your-customer (KYC) programs for financial services firms. She joined Fordham Law School from GE Capital, where she was the global compliance leader of AML and KYC. Prior to GE, she worked in various compliance and management positions for the Royal Bank of Scotland, BNP Paribas/Fortis, Fortis Bank, UBS, and Bear Stearns.

Scott Nathan
Accenture
Managing Director, Financial Intelligence and AML Utility Lead

Scott Nathan has over eighteen years of banking and financial crimes risk management experience. As part of the Accenture leadership team, he is focused on the development of a new Financial Intelligence practice deploying leading technology to change the paradigm of financial crimes compliance. Scott and the Accenture team have developed an innovative AML Analytics Utility leveraging the power of the Amazon cloud (AWS) and a community of participating financial institutions to reduce the cost of compliance, strengthen relationships with regulatory agencies and better support the end-user community (including intelligence and law enforcement) to protect national security.

Meryl Lutsky
New York State
Office of the Attorney General
Former Chief, Money Laundering Investigations Unit

Meryl Lutsky served as a prosecuting attorney for more than 20 years, the last 12 of which she spent leading the Statewide Crime Proceeds Strike Force and Money Laundering Unit for the New York State Attorney General’s Office. In this role, she created multi-agency and multi-disciplinary task forces consisting of local, state and federal attorneys, investigators, auditors and analysts, and partnered with state and federal banking regulators to identify, investigate, prosecute, and remediate complex Money Laundering crimes and violations of the Banking and Tax Laws, including those related to Cyber Hacking, Identity Theft, Human Trafficking, Public Corruption, etc.

Brian Price
Standard Charter
Program Director, Financial Crimes Compliance

Brian has been with Standard Chartered Bank for 25 years. He joined the Financial Crimes Compliance Analytics and Change team in 2015 and is responsible for Change Governance including audit and regulatory, external rules, operational risk, and policies and procedures. He previously held the position of Financial Controller for the Americas region and Acting Regional CFO. Brian joined the Bank as part of the American Express Bank acquisition and was the COO for AEB Global Financial Markets based in NY. He initially joined the Bank in the finance department where he was the Treasury Controller.
EXECUTIVE SUMMARY

THE NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES ("DFS") ISSUED ITS FINAL REGULATION ON BSA/AML TRANSACTION MONITORING AND OFAC FILTERING PROGRAMS. THE NEW REGULATION REQUIRES SENIOR OFFICERS OR THE BOARD OF INSTITUTIONS TO ANNUALLY CERTIFY THEIR ACCOUNTABILITY FOR THESE PROGRAMS

BACKGROUND

• The New York State DFS identified that weaknesses in Transaction Monitoring Programs and OFAC Filtering Programs in regulated institutions were attributed to a lack of robust governance, oversight, and accountability at senior levels.

• As a result the DFS adopted Part 504 of the New York State Banking Regulations which clarifies the required attributes or capabilities for these Programs and requires that the Board of Directors or Senior Officer(s) or a regulated institution annually certify compliance.

REQUIREMENT

• Part 504 of the DFS became effective January 2017. This requires all DFS regulated institutions to:
  • Install and maintain a risk-based BSA / AML Transaction Monitoring and OFAC Filtering Program.
  • Submit on an annual basis a “compliance finding” by the Board of Directors or Senior Officers to certify that the regulated institution is in compliance with Part 504.

• The first compliance findings are due April 2018. This will require regulated institutions to:
  1. Undertake comprehensive and holistic assessments of their transaction monitoring and filtering programs.
  2. Provide appropriate supporting evidence to demonstrate the effectiveness of the programs.
  3. Execute remedial efforts, material improvements, or redesigns to keep the programs in compliance.
  4. Implement governance processes for the annual certification.
DFS 504 COMPLIANCE TIMELINE

THE REGULATION WAS EFFECTIVE AS OF JANUARY 2017, WITH THE FIRST ANNUAL BOARD RESOLUTION OR COMPLIANCE FINDING DUE APRIL 2018. THIS MEANS THAT REGULATED INSTITUTIONS REQUIRE REPEATABLE CERTIFICATION PROCESSES

Jan. 2017: DFS 504 is effective. Regulated Institutions are required to prepare and submit Board or Senior Officer’s findings as per the requirements.

Jan. 1, 2017: DFS 504 is effective. Regulated Institutions are required to prepare and submit Board or Senior Officer’s findings as per the requirements.

Feb. 2018: Complete sub-certification and documentary evidence of compliance. First draft of Board Resolution.

Mar. 2018: Complete certification by the Board of Directors or Senior Officer(s).

April 2018: Submit certification to the regulator

Beyond: Start again !!!

Aug. 2017: Document and commence remedial efforts to address findings from DFS 504 assessment.

Mar. 2018: Complete certification by the Board of Directors or Senior Officer(s).

Aug. 2017: Document and commence remedial efforts to address findings from DFS 504 assessment.


Beyond…

COMMON CHALLENGES FOR CONSIDERATION

A NUMBER OF CHALLENGES EXIST THAT MUST BE ADDRESSED FOR REGULATED INSTITUTIONS TO MEET THEIR OBLIGATIONS UNDER DFS 504

PEOPLE & RESOURCES
- Few dedicated resources and limited capacity within BAU teams of regulated institutions to perform comprehensive review of the transaction monitoring and filtering program.
- Limited skills or experience within regulated institutions to implement material improvements or remedial initiatives to programs.

EVIDENCE
- Lack of a defined system of record or documentary repository dedicated to DFS 504 compliance.
- Lack of appropriate standards for evidencing data quality validation, model validation, and detection model optimization.

SYSTEMS & DATA
- Limited documentation and understanding on the completeness of end-to-end data lineage in detection systems.
- Limited integration of information from other programs to assist with transaction monitoring and sanctions filtering.

GOVERNANCE & OWNERSHIP
- Lack of an established process for certification to ensure accountability across relevant Functions and Business Units to the Board of Directors or Senior Officer(s).
- Unclear ownership and lack of a comprehensive execution plan to ensure accuracy, timeliness and completeness of the compliance finding.
As Process owner for both Transaction Monitoring and Transaction Screening, FCC (Financial Crime Compliance) will be the annual DFS 504 Certification signatory with Board level endorsement. The Certification process, however, is a Bank-wide effort as FCC, Data Management, IT, Risk Assessment, Model Governance, Data Analytics, Assurance, Group Internal Audit, Vendor Management and others necessarily come together to deliver an “effective” monitoring and filtering program.

- Patricia Sullivan
  
  Standard Chartered
  Regional Head,
  Financial Crime Compliance Americas
REGULATION 504 AND THE NYS PENAL LAW

EVEN THOUGH THE FINAL RULE DOES NOT EXPLICITLY REFER TO CRIMINAL PENALTIES NYSDFS HAD STATED THAT IF A PROGRAM IS NOT REASONABLY DESIGNED AND IF THE COMPLIANCE FINDING IS NOT BASED ON A REVIEW OF NECESSARY DOCUMENTS AND MATERIALS, AND IF THE COMPLIANCE FINDING WAS MADE WITH INTENT TO DECEIVE, THEN THE CERTIFYING INDIVIDUAL(S) MAY BE SUBJECT TO CRIMINAL PENALTIES

- Falsifying Business Records/Offering a False Instrument for Filing
  - 1st Degree (Class “E” Felony Crimes)
- Falsifying Business Records/Offering a False Instrument for Filing
  - 2nd Degree (Class “A” Misdemeanor Crimes)
- Conspiracy 5th Degree/Facilitation 4th Degree/Solicitation 4th Degree
  - All Class “A” Misdemeanor Crimes
- Conspiracy 6th Degree
  - Class “B” Misdemeanor Crime
- Solicitation 5th Degree
  - Violation (Not a Crime)
WHAT QUESTIONS DO YOU HAVE FOR OUR PANELISTS?
§ 504.1 Background.

The Department of Financial Services (the “Department”) has been involved in investigations into compliance by Regulated Institutions, as defined below, with applicable Bank Secrecy Act/Anti-Money Laundering laws and regulations1 (“BSA/AML”) and Office of Foreign Assets Control of the Treasury Department (“OFAC”)2 requirements implementing federal economic and trade sanctions.3

As a result of these investigations, the Department identified shortcomings in the transaction monitoring and filtering programs of these institutions attributable to a lack of robust governance, oversight, and accountability at senior levels. Based on not only this experience, but also its regular examinations for safety and soundness, along with other factors, the Department has reason to believe that financial institutions have shortcomings in their transaction monitoring and filtering programs.

As a result, the Department has determined to clarify the required attributes of a Transaction Monitoring and Filtering Program and to require that the Board of Directors or Senior Officer(s), as applicable, of each Regulated Institution submit to the Superintendent annually a Board

---

1 With respect to federal laws and regulations, see 31 U.S.C. § 5311, et seq. and 31 CFR Chapter X. For New York State regulations, see Part 115 (3 NYCRR 115), Part 116 (3 NYCRR 116), Part 416 (3 NYCRR 416) and Part 417 (3 NYCRR 417).
2 31 CFR part 501 et seq.
3 For information regarding the Unites States Code, the Code of Federal Regulations and the Federal Register, see Supervisory Policy G-1.
Resolution or Compliance Finding, as defined in this Part, confirming the steps taken to ascertain compliance by the Regulated Institution with this Part.

This regulation implements these requirements.

§ 504.2 Definitions.

The following definitions apply in this Part:

(a) “Annual Board Resolution or Senior Officer Compliance Finding” means a board resolution or senior officer(s) finding in the form set forth in Attachment A.

(b) “Bank Regulated Institutions” means all banks, trust companies, private bankers, savings banks, and savings and loan associations chartered pursuant to the New York Banking Law (the “Banking Law”) and all branches and agencies of foreign banking corporations licensed pursuant to the Banking Law to conduct banking operations in New York.

(c) “Board of Directors” means the governing board of every Regulated Institution or the functional equivalent if the Regulated Institution does not have a Board of Directors.

(d) “Nonbank Regulated Institutions” shall mean all check cashers and money transmitters licensed pursuant to the Banking Law.

(e) “Regulated Institutions” means all Bank Regulated Institutions and all Nonbank Regulated Institutions.

(f) “Risk Assessment” means an on-going comprehensive risk assessment, including an enterprise wide BSA/AML risk assessment, that takes into account the institution’s size, staffing, governance, businesses, services, products, operations, customers, counterparties, other relations and their locations, as well as the geographies and locations of its operations and business relations;

(g) “Senior Officer(s)” shall mean the senior individual or individuals responsible for the management, operations, compliance and/or risk of a Regulated Institution including a branch or agency of a foreign banking organization subject to this Part.

(h) “Suspicious Activity Reporting” means a report required pursuant to 31 U.S.C. § 5311 et seq. that identifies suspicious or potentially suspicious or illegal activities.

(i) “Transaction Monitoring Program” means a program that includes the attributes specified in Subdivisions (a), (c) and (d) of Section 504.3.

(j) “Filtering Program” means a program that includes the attributes specified in Subdivisions (b), (c) and (d) of Section 504.3.
(k) “Transaction Monitoring and Filtering Program” means a Transaction Monitoring Program, and a Filtering Program, collectively.

§ 504.3 Transaction Monitoring and Filtering Program Requirements.

(a) Each Regulated Institution shall maintain a Transaction Monitoring Program reasonably designed for the purpose of monitoring transactions after their execution for potential BSA/AML violations and Suspicious Activity Reporting, which system may be manual or automated, and which shall include the following attributes, to the extent they are applicable:

1. be based on the Risk Assessment of the institution;

2. be reviewed and periodically updated at risk-based intervals to take into account and reflect changes to applicable BSA/AML laws, regulations and regulatory warnings, as well as any other information determined by the institution to be relevant from the institution’s related programs and initiatives;

3. appropriately match BSA/AML risks to the institution’s businesses, products, services, and customers/counterparties;

4. BSA/AML detection scenarios with threshold values and amounts designed to detect potential money laundering or other suspicious or illegal activities;

5. end-to-end, pre-and post-implementation testing of the Transaction Monitoring Program, including, as relevant, a review of governance, data mapping, transaction coding, detection scenario logic, model validation, data input and Program output;

6. documentation that articulates the institution’s current detection scenarios and the underlying assumptions, parameters, and thresholds;

7. protocols setting forth how alerts generated by the Transaction Monitoring Program will be investigated, the process for deciding which alerts will result in a filing or other action, the operating areas and individuals responsible for making such a decision, and how the investigative and decision-making process will be documented; and

8. be subject to an on-going analysis to assess the continued relevancy of the detection scenarios, the underlying rules, threshold values, parameters, and assumptions.

(b) Each Regulated Institution shall maintain a Filtering Program, which may be manual or automated, reasonably designed for the purpose of interdicting transactions that are prohibited by OFAC, and which shall include the following attributes, to the extent applicable:

1. be based on the Risk Assessment of the institution;
2. be based on technology, processes or tools for matching names and accounts\(^4\), in each case based on the institution’s particular risks, transaction and product profiles;

3. end-to-end, pre- and post-implementation testing of the Filtering Program, including, as relevant, a review of data matching, an evaluation of whether the OFAC sanctions list and threshold settings map to the risks of the institution, the logic of matching technology or tools, model validation, and data input and Program output;

4. be subject to on-going analysis to assess the logic and performance of the technology or tools for matching names and accounts, as well as the OFAC sanctions list and the threshold settings to see if they continue to map to the risks of the institution; and

5. documentation that articulates the intent and design of the Filtering Program tools, processes or technology.

(c) Each Transaction Monitoring and Filtering Program shall require the following, to the extent applicable:

1. identification of all data sources that contain relevant data;

2. validation of the integrity, accuracy and quality of data to ensure that accurate and complete data flows through the Transaction Monitoring and Filtering Program;

3. data extraction and loading processes to ensure a complete and accurate transfer of data from its source to automated monitoring and filtering systems, if automated systems are used;

4. governance and management oversight, including policies and procedures governing changes to the Transaction Monitoring and Filtering Program to ensure that changes are defined, managed, controlled, reported, and audited;

5. vendor selection process if a third party vendor is used to acquire, install, implement, or test the Transaction Monitoring and Filtering Program or any aspect of it;

6. funding to design, implement and maintain a Transaction Monitoring and Filtering Program that complies with the requirements of this Part;

7. qualified personnel or outside consultant(s) responsible for the design, planning, implementation, operation, testing, validation, and on-going analysis of the Transaction Monitoring and Filtering Program, including automated systems if applicable, as well as case management, review and decision making with respect to generated alerts and potential filings; and

\(^4\) The technology used in this area may be based on automated tools that develop matching algorithms, such as those that use various forms of so-called “fuzzy logic” and culture-based name conventions to match names. This regulation does not mandate the use of any particular technology, only that the system or technology used must be reasonably designed to identify prohibited transactions.
8. periodic training of all stakeholders with respect to the Transaction Monitoring and Filtering Program.

(d) To the extent a Regulated Institution has identified areas, systems, or processes that require material improvement, updating or redesign, the Regulated Institution shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the Superintendent.

§ 504.4 Annual Board Resolution or Senior Officer(s) Compliance Finding.

To ensure compliance with the requirements of this Part, each Regulated Institution shall adopt and submit to the Superintendent a Board Resolution or Senior Officer(s) Compliance Finding in the form set forth in Attachment A by April 15th of each year. Each Regulated Institution shall maintain for examination by the Department all records, schedules and data supporting adoption of the Board Resolution or Senior Officer(s) Compliance Finding for a period of five years.

§ 504.5 Penalties/Enforcement Actions.

This regulation will be enforced pursuant to, and is not intended to limit, the Superintendent’s authority under any applicable laws.

§ 504.6 Effective Date.

This Part shall be effective January 1, 2017. Regulated Institutions will be required to prepare and submit to the Superintendent Annual Board Resolutions or Senior Officer(s) Compliance Findings under § 504.4 commencing April 15, 2018.
ATTACHMENT A

____________________________________________
(Regulated Institution Name)

APRIL 15, 20____

Annual Board Resolution or Senior Officer(s) Compliance Finding For Bank Secrecy Act/Anti-
Money Laundering and Office of Foreign Asset Control Transaction Monitoring and Filtering
Program

Whereas, in compliance with the requirements of the New York State Department of Financial Services (the “Department”) that each Regulated Institution maintain Transaction Monitoring and Filtering Program in compliance with Section 504.3; and

Whereas, Section 504.4 requires that the Board of Directors or a Senior Officer(s), as appropriate, adopt and submit to the Superintendent a Board Resolution or Senior Officer Compliance Finding confirming its or such individual’s findings that the Regulated Institution is in compliance with Section 504.3 of this Part 504;

NOW, THEREFORE, the Board of Directors or Senior Officer certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary to adopt this Board Resolution or Senior Officer Compliance Finding;

(2) The Board of Directors or Senior Officer(s) has taken all steps necessary to confirm that (name of Regulated Institution) has a Transaction Monitoring and Filtering Program that complies with the provisions of Section 504.3; and

(3) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Transaction Monitoring and the Filtering Program of (name of Regulated Institution) as of ____________ (date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended ________ (year for which Board Resolution or Compliance Finding is provided) complies with Section 504.3.
Signed by each member of the Board of Directors or Senior Officer(s)

(Name)____________________________                Date:
FREQUENTLY ASKED QUESTIONS REGARDING 3 NYCRR 504

1. What as of date should a Regulated Institution use for the “as of” date for its transaction monitoring and filtering program certification?

Regulated Institutions should submit the required certification covering the prior calendar year by April 15 of each year.

2. May a Regulated Institution submit a certification under 3 NYCRR 504.7 if it is not yet in compliance with the requirements of Part 504?

The Department expects full compliance with the regulation. A Regulated Institution may not submit a certification under 3 NYCRR 504.7 unless the Regulated Institution is in compliance with the requirements of Part 504 as of the effective date of the certification.

3. Should a Regulated Institution send additional documentation along with the certification proving that the system is in compliance?

The Regulated Institution must submit the compliance certification to the Department and is not required to submit explanatory or additional materials with the certification. The certification is intended as a stand-alone document required by the regulation. The Department also expects that the Regulated Institution maintains the documents and records necessary that support the certification, should the Department request such information in the future. Likewise, under 3 NYCRR 504.3(d), to the extent a Regulated Institution has identified areas, systems, or processes that require material improvement, updating or redesign, the Regulated Institution must document such efforts and maintain such schedules and documentation for inspection during the examination process or as otherwise requested by the Department.

4. Does the Department require a pre-implementation testing for systems the Regulated Institutions used that were operational prior to the Regulation?

The Department will not require full end-to-end, pre implementation testing of systems that the Regulated Institution uses that were operational prior to the effective date of the regulation, as is required when adopting new systems. However, under 3 NYCRR 504.3(a)(2), Regulated Entities’ systems and programs must “be reviewed and periodically updated at risk-based intervals” and thus Regulated Institutions are expected to conduct periodic risk based systems testing and data validation on all systems that support the transaction monitoring and filtering program.

5. Does the Department require the Regulated Institution to conduct a vendor selection for the systems that are already in place prior to the Regulation?

The Department does not require a Regulated Institution to conduct a vendor selection process for vendors that were engaged prior to the effective date of the regulation, as is now required when hiring a new vendor to acquire, install, implement or test the transaction monitoring and filtering program. However, on an ongoing basis, 3 NYCRR 504.3(c)(7) requires Regulated Institutions to engage qualified personnel or outside consultants for these purposes and as such Regulated Entities should have processes in place to confirm that the personnel and vendors it has engaged to execute its transaction monitoring and filtering program are qualified and competent.
NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
23 NYCRR 500

CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

I, Maria T. Vullo, Superintendent of Financial Services, pursuant to the authority granted by sections 102, 201, 202, 301, 302 and 408 of the Financial Services Law, do hereby promulgate Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, to take effect March 1, 2017, to read as follows:

(ALL MATTER IS NEW)

Section 500.00 Introduction.

The New York State Department of Financial Services (“DFS”) has been closely monitoring the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. Recently, cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data. Cybercriminals can cause significant financial losses for DFS regulated entities as well as for New York consumers whose private information may be revealed and/or stolen for illicit purposes. The financial services industry is a significant target of cybersecurity threats. DFS appreciates that many firms have proactively increased their cybersecurity programs with great success.

Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances. Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization’s cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity’s cybersecurity program must ensure the safety and soundness of the institution and protect its customers.

It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs. The number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark. Adoption of the program outlined in these regulations is a priority for New York State.

Section 500.01 Definitions.

For purposes of this Part only, the following definitions shall apply:

(a) **Affiliate** means any Person that controls, is controlled by or is under common control with another Person. For purposes of this subsection, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise.
(b) **Authorized User** means any employee, contractor, agent or other Person that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity.

(c) **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.

(d) **Cybersecurity Event** means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.

(e) **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.

(f) **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.

(g) **Nonpublic Information** shall mean all electronic information that is not Publicly Available Information and is:

1. Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity;

2. Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers’ license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual’s financial account, or (v) biometric records;

3. Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.
(h) *Penetration Testing* means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside the Covered Entity’s Information Systems.

(i) *Person* means any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association.

(j) *Publicly Available Information* means any information that a Covered Entity has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law.

(1) For the purposes of this subsection, a Covered Entity has a reasonable basis to believe that information is lawfully made available to the general public if the Covered Entity has taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

(k) *Risk Assessment* means the risk assessment that each Covered Entity is required to conduct under section 500.09 of this Part.

(l) *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.

(m) *Senior Officer(s)* means the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity, including a branch or agency of a foreign banking organization subject to this Part.

(n) *Third Party Service Provider(s)* means a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.

**Section 500.02 Cybersecurity Program.**

(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity’s Information Systems.

(b) The cybersecurity program shall be based on the Covered Entity’s Risk Assessment and designed to perform the following core cybersecurity functions:

(1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity’s Information Systems;
(2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity’s Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;

(3) detect Cybersecurity Events;

(4) respond to identified or detected Cybersecurity Events to mitigate any negative effects;

(5) recover from Cybersecurity Events and restore normal operations and services; and

(6) fulfill applicable regulatory reporting obligations.

(c) A Covered Entity may meet the requirement(s) of this Part by adopting the relevant and applicable provisions of a cybersecurity program maintained by an Affiliate, provided that such provisions satisfy the requirements of this Part, as applicable to the Covered Entity.

(d) All documentation and information relevant to the Covered Entity’s cybersecurity program shall be made available to the superintendent upon request.

Section 500.03 Cybersecurity Policy.

Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity’s board of directors (or an appropriate committee thereof) or equivalent governing body, 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 be based on the Covered Entity’s Risk Assessment and address the following areas to the extent applicable to the Covered Entity’s operations:

(a) information security;

(b) data governance and classification;

(c) asset inventory and device management;

(d) access controls and identity management;

(e) business continuity and disaster recovery planning and resources;

(f) systems operations and availability concerns;

(g) systems and network security;

(h) systems and network monitoring;

(i) systems and application development and quality assurance;
(j) physical security and environmental controls;

(k) customer data privacy;

(l) vendor and Third Party Service Provider management;

(m) risk assessment; and

(n) incident response.

Section 500.04 Chief Information Security Officer.

(a) Chief Information Security Officer. Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity’s cybersecurity program and enforcing its cybersecurity policy (for purposes of this Part, “Chief Information Security Officer” or “CISO”). The CISO may be employed by the Covered Entity, one of its Affiliates or a Third Party Service Provider. To the extent this requirement is met using a Third Party Service Provider or an Affiliate, the Covered Entity shall:

(1) retain responsibility for compliance with this Part;

(2) designate a senior member of the Covered Entity’s personnel responsible for direction and oversight of the Third Party Service Provider; and

(3) require the Third Party Service Provider to maintain a cybersecurity program that protects the Covered Entity in accordance with the requirements of this Part.

(b) Report. The CISO of each Covered Entity shall report in writing at least annually to the Covered Entity’s board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity’s cybersecurity program. The CISO shall report on the Covered Entity’s cybersecurity program and material cybersecurity risks. The CISO shall consider to the extent applicable:

(1) the confidentiality of Nonpublic Information and the integrity and security of the Covered Entity’s Information Systems;

(2) the Covered Entity’s cybersecurity policies and procedures;

(3) material cybersecurity risks to the Covered Entity;

(4) overall effectiveness of the Covered Entity’s cybersecurity program; and

(5) material Cybersecurity Events involving the Covered Entity during the time period addressed by the report.

Section 500.05 Penetration Testing and Vulnerability Assessments.
The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity’s Risk Assessment, designed to assess the effectiveness of the Covered Entity’s cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct:

(a) annual Penetration Testing of the Covered Entity’s Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and

(b) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity’s Information Systems based on the Risk Assessment.

Section 500.06 Audit Trail.

(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment:

(1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and

(2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.

(b) Each Covered Entity shall maintain records required by section 500.06(a)(1) of this Part for not fewer than five years and shall maintain records required by section 500.06(a)(2) of this Part for not fewer than three years.

Section 500.07 Access Privileges.

As part of its cybersecurity program, based on the Covered Entity’s Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.

Section 500.08 Application Security.

(a) Each Covered Entity’s cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity’s technology environment.

(b) All such procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity.

Section 500.09 Risk Assessment.
(a) Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity’s Information Systems sufficient to inform the design of the cybersecurity program as required by this Part. Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity’s Information Systems, Nonpublic Information or business operations. The Covered Entity’s Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity’s business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems.

(b) The Risk Assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:

(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity;

(2) criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity’s Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks; and

(3) requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.

Section 500.10 Cybersecurity Personnel and Intelligence.

(a) Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in section 500.04(a) of this Part, each Covered Entity shall:

(1) utilize qualified cybersecurity personnel of the Covered Entity, an Affiliate or a Third Party Service Provider sufficient to manage the Covered Entity’s cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in section 500.02(b)(1)-(6) of this Part;

(2) provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and

(3) verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

(b) A Covered Entity may choose to utilize an Affiliate or qualified Third Party Service Provider to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in section 500.11 of this Part.

Section 500.11 Third Party Service Provider Security Policy.

(a) Third Party Service Provider Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible
to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable:

(1) the identification and risk assessment of Third Party Service Providers;

(2) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity;

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and

(4) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

(b) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers including to the extent applicable guidelines addressing:

(1) the Third Party Service Provider’s policies and procedures for access controls, including its use of Multi-Factor Authentication as required by section 500.12 of this Part, to limit access to relevant Information Systems and Nonpublic Information;

(2) the Third Party Service Provider’s policies and procedures for use of encryption as required by section 500.15 of this Part to protect Nonpublic Information in transit and at rest;

(3) notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity’s Information Systems or the Covered Entity’s Nonpublic Information being held by the Third Party Service Provider; and

(4) representations and warranties addressing the Third Party Service Provider’s cybersecurity policies and procedures that relate to the security of the Covered Entity’s Information Systems or Nonpublic Information.

(c) Limited Exception. An agent, employee, representative or designee of a Covered Entity who is itself a Covered Entity need not develop its own Third Party Information Security Policy pursuant to this section if the agent, employee, representative or designee follows the policy of the Covered Entity that is required to comply with this Part.

Section 500.12 Multi-Factor Authentication.

(a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.

(b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity’s internal networks from an external network, unless the Covered Entity’s CISO has approved in writing the use of reasonably equivalent or more secure access controls.
Section 500.13 Limitations on Data Retention.

As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information identified in section 500.01(g)(2)-(3) of this Part that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Section 500.14 Training and Monitoring.

As part of its cybersecurity program, each Covered Entity shall:

(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users; and

(b) provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.

Section 500.15 Encryption of Nonpublic Information.

(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.

(1) To the extent a Covered Entity determines that encryption of Nonpublic Information in transit over external networks is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity’s CISO.

(2) To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity’s CISO.

(b) To the extent that a Covered Entity is utilizing compensating controls under (a) above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.

Section 500.16 Incident Response Plan.

(a) As part of its cybersecurity program, each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity’s Information Systems or the continuing functionality of any aspect of the Covered Entity’s business or operations.

(b) Such incident response plan shall address the following areas:

(1) the internal processes for responding to a Cybersecurity Event;
(2) the goals of the incident response plan;

(3) the definition of clear roles, responsibilities and levels of decision-making authority;

(4) external and internal communications and information sharing;

(5) identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;

(6) documentation and reporting regarding Cybersecurity Events and related incident response activities; and

(7) the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

Section 500.17 Notices to Superintendent.

(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following:

1) Cybersecurity Events impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or

2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

(b) Annually each Covered Entity shall submit to the superintendent a written statement covering the prior calendar year. This statement shall be submitted by February 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. To the extent a Covered Entity has identified areas, systems or processes that require material improvement, updating or redesign, the Covered Entity shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the superintendent.

Section 500.18 Confidentiality.

Information provided by a Covered Entity pursuant to this Part is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law.

Section 500.19 Exemptions.

(a) Limited Exemption. Each Covered Entity with:
(1) fewer than 10 employees, including any independent contractors, of the Covered Entity or its Affiliates located in New York or responsible for business of the Covered Entity, or

(2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity and its Affiliates, or

(3) less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates,

shall be exempt from the requirements of sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(b) An employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity.

(c) A Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(d) A Covered Entity under Article 70 of the Insurance Law that does not and is not required to directly or indirectly control, own, access, generate, receive or possess Nonpublic Information other than information relating to its corporate parent company (or Affiliates) shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(e) A Covered Entity that qualifies for any of the above exemptions pursuant to this section shall file a Notice of Exemption in the form set forth as Appendix B within 30 days of the determination that the Covered Entity is exempt.

(f) The following Persons are exempt from the requirements of this Part, provided such Persons do not otherwise qualify as a Covered Entity for purposes of this Part: Persons subject to Insurance Law section 1110; Persons subject to Insurance Law section 5904; and any accredited reinsurer or certified reinsurer that has been accredited or certified pursuant to 11 NYCRR 125.

(g) In the event that a Covered Entity, as of its most recent fiscal year end, ceases to qualify for an exemption, such Covered Entity shall have 180 days from such fiscal year end to comply with all applicable requirements of this Part.

Section 500.20 Enforcement.

This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent’s authority under any applicable laws.

Section 500.21 Effective Date.
This Part will be effective March 1, 2017. Covered Entities will be required to annually prepare and submit to the superintendent a Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations under section 500.17(b) of this Part commencing February 15, 2018.

Section 500.22 Transitional Periods.

(a) Transitional Period. Covered Entities shall have 180 days from the effective date of this Part to comply with the requirements set forth in this Part, except as otherwise specified.

(b) The following provisions shall include additional transitional periods. Covered Entities shall have:

(1) One year from the effective date of this Part to comply with the requirements of sections 500.04(b), 500.05, 500.09, 500.12, and 500.14(b) of this Part.

(2) Eighteen months from the effective date of this Part to comply with the requirements of sections 500.06, 500.08, 500.13, 500.14(a) and 500.15 of this Part.

(3) Two years from the effective date of this Part to comply with the requirements of section 500.11 of this Part.

Section 500.23 Severability.

If any provision of this Part or the application thereof to any Person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or the application thereof to other Persons or circumstances.
(Covered Entity Name)

February 15, 20____

Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity) as of __________(date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended__(year for which Board Resolution or Compliance Finding is provided) complies with Part ___.

Signed by the Chairperson of the Board of Directors or Senior Officer(s)

(Name)_________________________________________ Date: ____________________

[DFS Portal Filing Instructions]
(Covered Entity Name)

(Date)____________

Notice of Exemption

In accordance with 23 NYCRR § 500.19(e), (Covered Entity Name) hereby provides notice that (Covered Entity Name) qualifies for the following Exemption(s) under 23 NYCRR § 500.19 (check all that apply):

☐ Section 500.19(a)(1)
☐ Section 500.19(a)(2)
☐ Section 500.19(a)(3)
☐ Section 500.19(b)
☐ Section 500.19(c)
☐ Section 500.19(d)

If you have any question or concerns regarding this notice, please contact:

(Insert name, title, and full contact information)

(Name)_________________________________________ Date: ________________
(Title)
(Covered Entity Name)

[DFS Portal Filing Instructions]
FREQUENTLY ASKED QUESTIONS REGARDING 23 NYCRR PART 500

Effective March 1, 2017, the Superintendent of Financial Services promulgated 23 NYCRR Part 500, a regulation establishing cybersecurity requirements for financial services companies. The following provides answers to frequently asked questions concerning 23 NYCRR Part 500. Terms used below have the meanings assigned to them in 23 NYCRR 500.01. Please note that the Department may revise or update the below information from time to time, as appropriate.

1. Assuming there is no continuous monitoring under 23 NYCRR Section 500.05, does the Department require that a Covered Entity complete a Penetration Test and vulnerability assessments by March 1, 2018?

The Regulation requires Covered Entities to have a plan in place that provides for Penetration Testing to be done as appropriate to address the risks of the Covered Entity. Such plan must encompass Penetration Testing at least annually and bi-annual vulnerability assessments, but the first annual Penetration Testing and first vulnerability assessment need not have been concluded before March 1, 2018 under Section 500.05. The Department expects all institutions with no continuous monitoring to complete robust Penetration Testing and vulnerability assessment in a timely manner as they are a crucial component of a cybersecurity program.

2. If Covered Entity A utilizes Covered Entity B (not related to Covered Entity A) as a Third Party Service Provider, and Covered Entity B provides Covered Entity A with evidence of its Certification of Compliance with NYSDFS Cybersecurity Regulations, could that be considered adequate due diligence under the due diligence process required by Section 500.11(a)(3)?

No. The Department emphasizes the importance of a thorough due diligence process in evaluating the cybersecurity practices of a Third Party Service Provider. Solely relying on the Certification of Compliance will not be adequate due diligence. Covered Entities must assess the risks each Third Party Service Provider poses to their data and systems and effectively address those risks. The Department has provided a two year transitional period to address these risks and expects Covered Entities to have completed a thorough due diligence process on all Third Party Service Providers by March 1, 2019.

3. Does a Covered Entity need to amend its Notice of Exemption in the event of changes after the initial submission (e.g., name changes or changes to the applicable exemption(s))?

If there are changes, the Covered Entity should submit a new Notice of Exemption, which would not be considered an amendment to the original submission. For example, if a Covered Entity originally submitted a Notice of Exemption stating that it qualified for exemptions under Sections 500.19(b) and 500.19(a)(1), but it now only qualifies for a Section 500.19(a)(1) exemption, then the Covered Entity must submit a new Notice of Exemption with the correct information.

The Department also emphasizes that Notices of Exemption should be filed electronically via the DFS Web Portal http://www.dfs.ny.gov/about/cybersecurity. The Covered Entity should utilize the account that they used to file the original Notice of Exemption or create a new account if an individual filing was previously not made. Filings made through the DFS Web Portal are preferred to alternative filing mechanisms because the DFS Web Portal provides a secure reporting tool to facilitate compliance with the filing requirements of 23 NYCRR Part 500.

4. Should a Covered Entity send supporting documentation along with the Certification of Compliance?

The Covered Entity must submit the compliance certification to the Department and is not required to submit explanatory or additional materials with the certification. The certification is intended as a stand-alone document required by the regulation. The Department also expects that the Covered Entity maintains the documents and records necessary that support the certification, should the Department request such information in the future. Likewise, under 23 NYCRR Section 500.17, to the extent a Covered Entity has identified areas, systems, or processes that require material improvement, updating or redesign, the Covered Entity must document such efforts and maintain such schedules and documentation for inspection during the examination process or as otherwise requested by the Department.

5. Is a Covered Entity entitled to an exemption under Section 500.19(b) if that Covered Entity is an employee, agent, representative or designee of more than one other Covered Entity?

Section 500.19(b) states that a Covered Entity who is an "employee, agent, representative or designee of a Covered Entity . . . is exempt from" 23 NYCRR Part 500 and "need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity" (emphasis added). This exemption requires an entire employee, agent, representative or designee to be fully covered by the program of another Covered Entity.
Therefore, a Covered Entity who is an employee, agent, representative or designee of more than one other Covered Entity will only qualify for a Section 500.19(b) exemption where the cybersecurity program of at least one of its parent Covered Entities fully covers all aspects of the employee’s, agent’s, representative’s or designee’s business.

6. Does a Covered Entity that qualifies for an exemption under 23 NYCRR Section 500.19(b) need to file a notice of exemption?

Yes. 23 NYCRR 500.19 subsections (a) through (d) set forth certain limited exemptions from different requirements of Part 500. Pursuant to 23 NYCRR Section 500.19(e): "[a] Covered Entity that qualifies for any of the above exemptions pursuant to this section shall file a Notice of Exemption" (emphasis added).

7. Under Section 500.04(b), can the requirement that the CISO report in writing at least annually "to the Covered Entity's board of directors" (the "board") be met by reporting to an authorized subcommittee of the board?

No. The Department emphasizes that a well-informed board is a crucial part of an effective cybersecurity program and the CISO’s reporting to the full board is important to enable the board to assess the Covered Entity’s governance, funding, structure and effectiveness as well as compliance with 23 NYCRR Part 500 or other applicable laws or regulations.

8. Can a Covered Entity file a notice of exemption on behalf of its employees or agents?

By permission, the Department will approve certain Covered Entities to file notices of exemption on behalf of their employees or captive agents who are also Covered Entities. This option will only be available for filings of 50 or more employees or captive agents and only if all employees or captive agents qualify for the same exemptions. Covered Entities with over 50 employees or agents on whose behalf they have authority to file should contact the Department at CyberRegComments@dfs.ny.gov from the email to which your Cybersecurity portal account is associated with the following instructions. The Department will coordinate with the Covered Entity to submit a one-time filing form to effectuate an exemption filing for multiple covered entities. On the spreadsheet, the submitter will need to provide the first and last name, DFS identification number, type of license, and email for every employee or captive agent. After approval, the Department will send more detailed instructions and the exemption spreadsheet. In the event that there is a need for additional names or captive agents after the initial submission, the submitter will be able to submit a supplemental form through the portal. The Department emphasizes that the employee or captive agent, for whom the Covered Entity is filing, continues to be ultimately responsible in ensuring compliance with 23 NYCRR Part 500. It remains the responsibility of the employee or captive agent to notify the Department of any changes in their status.

9. When is an unsuccessful attack a Cybersecurity Event that has or had “a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity” under the reporting requirements of 23 NYCRR Section 500.17(a)(2)?

The Department recognizes that Covered Entities are regularly subject to many attempts to gain unauthorized access to, disrupt or misuse Information Systems and the information stored on them, and that many of these attempts are thwarted by the Covered Entities’ cybersecurity programs. The Department anticipates that most unsuccessful attacks will not be reportable, but seeks the reporting of those unsuccessful attacks that, in the considered judgment of the Covered Entity, are sufficiently serious to raise a concern. For example, notice to the Department under 23 NYCRR Section 500.17(a)(2) would generally not be required if, consistent with its Risk Assessment, a Covered Entity makes a good faith judgment that the unsuccessful attack was of a routine nature.

The Department believes that analysis of unsuccessful threats is critically important to the ongoing development and improvement of cybersecurity programs, and Covered Entities are encouraged to continually develop their threat assessment programs. Notice of the especially serious unsuccessful attacks may be useful to the Department in carrying out its broader supervisory responsibilities, and the knowledge shared through such notice can be used to timely improve cybersecurity generally across the industries regulated by the Department. Accordingly, Covered Entities are requested to notify the Department of those unsuccessful attacks that appear particularly significant based on the Covered Entity’s understanding of the risks it faces. For example, in making a judgment as to whether a particular unsuccessful attack should be reported, a Covered Entity might consider whether handling the attack required measures or resources well beyond those ordinarily used by the Covered Entity, like exceptional attention by senior personnel or the adoption of extraordinary non-routine precautionary steps.

The Department recognizes that Covered Entities’ focus should be on preventing cybersecurity attacks and improving systems to protect the institution and its customers. The Department’s notice requirement is intended to facilitate information sharing about serious events that threaten an institution’s integrity and that may be relevant to the Department’s overall supervision of the financial services industries. The Department trusts that Covered Entities will exercise appropriate judgment as to which unsuccessful attacks must be reported and does not intend to penalize Covered Entities for the exercise of honest, good faith judgment.

10. Are the New York branches of out-of-state domestic banks required to comply with 23 NYCRR Part 500?

New York is a signatory to the Nationwide Cooperative Agreement, Revised as of December 9, 1997 (the “Agreement”), an agreement among state banking regulators that addresses supervision in an interstate branching environment. Pursuant to the Agreement, the home state of a state-chartered bank with a branch or branches in New York under Article V-C of the New York Banking Law is primarily responsible for supervising such state-chartered bank, including its New York branches. In keeping with the Agreement’s goals of interstate coordination and cooperation with respect to the supervision and examination of bank branches, including compliance with applicable laws, DFS will defer to the home state supervisor for supervision and examination of the New York branches, with the understanding that DFS is available to coordinate and work with the home state in such supervision and examination. DFS notes that New York branches are required to comply with New York state law, and DFS maintains the right to examine branches located in New York. With respect to DFS’s cybersecurity regulation, given the ever-increasing cybersecurity risks that financial institutions face, DFS strongly encourages all financial institutions, including New York...
branches of out-of-state domestic banks, to adopt cybersecurity protections consistent with the safeguards and protections of 23 NYCRR Part 500.

11. How must a Covered Entity address cybersecurity issues with respect to its subsidiaries and other affiliates?

When a subsidiary or other affiliate of a Covered Entity presents risks to the Covered Entity’s Information Systems or the Nonpublic Information stored on those Information Systems, those risks must be evaluated and addressed in the Covered Entity’s Risk Assessment, cybersecurity program and cybersecurity policies (see 23 NYCRR Sections 500.09, 500.02 and 500.03, respectively). Other regulatory requirements may also apply, depending on the individual facts and circumstances.

12. If a Covered Entity qualifies for a limited exemption, does it need to comply with 23 NYCRR Part 500?

The exemptions listed in 23 NYCRR Part 500.19 are limited in scope. These exemptions have been tailored to address particular circumstances and include requirements that the Department believes are necessary for these exempted entities. As such, Covered Entities that qualify for those exemptions are only exempt from complying with certain provisions as set forth in the regulation, but must comply with the sections listed in the exemption that applies to that Covered Entity.

13. Under 23 NYCRR 500.17(a), is a Covered Entity required to give notice to the Department when a Cybersecurity Event involves harm to consumers?

Yes. 23 NYCRR 500.17(a) must be read in combination with other laws and regulations that apply to consumer privacy. Under 23 NYCRR 500.17(a)(1), a Covered Entity must give notice to the Department of any Cybersecurity Event “of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body,” which includes many Cybersecurity Events that involve consumer harm, whether actual or potential. To offer just one example, New York’s information security breach and notification law requires notices to affected consumers and to certain government bodies following a data breach. Under 23 NYCRR 500.17(a)(1), when such a data breach constitutes a Cybersecurity Event, it must also be reported to the Department.

In addition, under 23 NYCRR 500.17(a)(2), Cybersecurity Events must be reported to the Department if they “have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.” To the extent a Cybersecurity Event involves material consumer harm, it is covered by this provision.

14. Is a Covered Entity required to give notice to consumers affected by a Cybersecurity Event?

New York’s information security breach and notification law (General Business Law Section 899-aa), requires notice to consumers who have been affected by cybersecurity incidents. Further, under 23 NYCRR Part 500, a Covered Entity’s cybersecurity program and policy must address, to the extent applicable, consumer data privacy and other consumer protection issues. Additionally, Part 500 requires that Covered Entities address as part of their incident response plans external communications in the aftermath of a breach, which includes communication with affected customers. Thus, a Covered Entity’s cybersecurity program and policies will need to address notice to consumers in order to be consistent with the risk-based requirements of 23 NYCRR Part 500.

15. May a Covered Entity adopt portions of an Affiliate’s cybersecurity program without adopting all of it?

A Covered Entity may adopt an Affiliate’s cybersecurity program in whole or in part, as long as the Covered Entity’s overall cybersecurity program meets all requirements of 23 NYCRR Part 500. The Covered Entity remains responsible for full compliance with the requirements of 23 NYCRR Part 500. To the extent a Covered Entity relies on an Affiliate’s cybersecurity program in whole or in part, that program must be made available for examination by the Department.

16. May the certification requirement of 23 NYCRR 500.17(b) be met by an Affiliate?

No. Each Covered Entity is required to annually certify its compliance with Part 500 as required by 23 NYCRR 500.17(b).

17. To the extent a Covered Entity uses an employee of an Affiliate as its Chief Information Security Officer (“CISO”), is the Covered Entity required to satisfy the requirements of 23 NYCRR 500.04(a)(2)-(3)?

To the extent a Covered Entity utilizes an employee of an Affiliate to serve as the Covered Entity’s CISO for purposes of 23 NYCRR 500.04(a), the Affiliate is not considered a Third Party Service Provider for purposes of 23 NYCRR 500.04(a)(2)-(3). However, the Covered Entity retains full responsibility for compliance with the requirements of 23 NYCRR Part 500 at all times, including ensuring that the CISO responsible for the Covered Entity is performing the duties consistent with this Part.

18. Are the DFS-authorized New York branches, agencies and representative offices of out-of-country foreign banks required to comply with 23 NYCRR Part 500?

Yes. It is further noted that, in such cases, only the Information Systems supporting the branch, agency or representative office, and the Nonpublic Information of the branch, agency or representative office are subject to the applicable requirements of 23 NYCRR Part 500, whether through the branch’s, agency’s or representative office’s development and implementation of its own cybersecurity program or through the adoption of an Affiliate’s cybersecurity program.

19. Where interrelated requirements under 23 NYCRR Part 500 are subject to different transitional periods, when and to what extent are Covered Entities required to comply with currently applicable requirements that are impacted by separate requirements for which the applicable transitional period has not yet ended?

Covered Entities have 180 days from the March 1, 2017, effective date to come into compliance with the requirements of 23 NYCRR Part 500 unless otherwise specified in 23 NYCRR 500.22. While complying with currently applicable requirements under the final rule, Covered Entities are generally not required to comply with, or incorporate into their cybersecurity programs, provisions of the regulation for which the applicable transitional period has not yet ended. For example, while Covered Entities will be required to have a cybersecurity program as well as policies and procedures in place by August 28, 2017, the Department
recognizes that in some cases there may be updates and revisions thereafter that incorporate the results of a Risk Assessment later conducted, or other elements of Part 500 that are subject to longer transitional periods.

20. Is a Covered Entity required to certify compliance with all the requirements of 23 NYCRR 500 on February 15, 2018?

Covered Entities are required to submit the first certification under 23 NYCRR 500.17(b) by February 15, 2018. This initial certification applies to and includes all requirements of 23 NYCRR Part 500 for which the applicable transitional period under 23 NYCRR 500.22 has terminated prior to February 15, 2018. Accordingly, Covered Entities will not be required to submit certification of compliance with the requirements of 23 NYCRR 500.04(b), 500.05, 500.06, 500.08, 500.09, 500.12, 500.13, 500.14 and 500.15 until February 15, 2019, and certification of compliance with 23 NYCRR 500.11 until February 15, 2020.

21. May a Covered Entity submit a certification under 23 NYCRR 500.17(b) if it is not yet in compliance with all applicable requirements of Part 500?

The Department expects full compliance with this regulation. A Covered Entity may not submit a certification under 23 NYCRR 500.17(b) unless the Covered Entity is in compliance with all applicable requirements of Part 500 at the time of certification. To the extent a particular requirement of Part 500 is subject to an ongoing transitional period under 23 NYCRR 500.22 at the time of certification, that requirement would not be considered applicable for purposes of a certification under 23 NYCRR 500.17(b).

22. What constitutes “continuous monitoring” for purposes of 23 NYCRR 500.05?

Effective continuous monitoring could be attained through a variety of technical and procedural tools, controls and systems. There is no specific technology that is required to be used in order to have an effective continuous monitoring program. Effective continuous monitoring generally has the ability to continuously, on an ongoing basis, detect changes or activities within a Covered Entity’s Information Systems that may create or indicate the existence of cybersecurity vulnerabilities or malicious activity. In contrast, non-continuous monitoring of Information Systems, such as through periodic manual review of logs and firewall configurations, would not be considered to constitute “effective continuous monitoring” for purposes of 23 NYCRR 500.05.

23. When is a Covered Entity required to report a Cybersecurity Event under 23 NYCRR 500.17(a)?

23 NYCRR 500.17(a) requires Covered Entities to notify the superintendent of certain Cybersecurity Events as promptly as possible but in no event later than 72 hours from a determination that a reportable Cybersecurity Event has occurred. A Cybersecurity Event is reportable if it falls into at least one of the following categories:

- the Cybersecurity Event impacts the Covered Entity and notice of it is required to be provided to any government body, self-regulatory agency or any other supervisory body; or
- the Cybersecurity Event has a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

An attack on a Covered Entity may constitute a reportable Cybersecurity Event even if the attack is not successful.

24. How should a Covered Entity submit Notices of Exemption, Certifications of Compliance and Notices of Cybersecurity Events?

Cybersecurity Notices of Exemption, Certifications of Compliance, and Notices of Cybersecurity Events should be filed electronically via the DFS Web Portal http://www.dfs.ny.gov/about/cybersecurity. You will first be prompted to create an account and log in to the DFS Web Portal, then directed to the filing interface. Filings made through the DFS Web Portal are preferred for alternative filing mechanisms because the DFS Web Portal provides a secure reporting tool to facilitate compliance with the filing requirements of 23 NYCRR Part 500.

25. Can an entity be both a Covered Entity and a Third Party Service Provider under 23 NYCRR Part 500?

Yes. If an entity is both a Covered Entity and a Third Party Service Provider, the entity is responsible for meeting the requirements of 23 NYCRR Part 500 as a Covered Entity.

26. Are all Third Party Service Providers required to implement Multi-Factor Authentication and encryption when dealing with a Covered Entity?

23 NYCRR 500.11, among other things, generally requires a Covered Entity to develop and implement written policies and procedures designed to ensure the security of the Covered Entity’s Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers. 23 NYCRR 500.11(b) requires a Covered Entity to include in those policies and procedures guidelines, as applicable, addressing certain enumerated issues. Accordingly, 23 NYCRR 500.11(b) requires Covered Entities to make a risk assessment regarding the appropriate controls for Third Party Service Providers based on the individual facts and circumstances presented and does not create a one-size-fits-all solution.
The _____ count is Criminal Solicitation in the Fourth Degree.

Under our law, a person is guilty of Criminal Solicitation in the Fourth Degree when, with intent that another person engage in conduct constituting a felony, he or she solicits, requests, commands, importunes or otherwise attempts to cause such other person to engage in such conduct.

The term "intent" used in this definition has its own special meaning in our law. I will now give you the meaning of that term.

INTENT means conscious objective or purpose.¹ Thus, a person acts with the intent that another person engage in conduct constituting a felony when his or her conscious objective or purpose is that such other person engage in such conduct.

Under our law, (specify the solicited felony) is a felony. A person is guilty of (specify the solicited felony), when (read the applicable portion of the statutory definition of the solicited felony).

Under our law, it is no defense to a prosecution for criminal solicitation that the person solicited could not be guilty of the crime solicited owing to criminal irresponsibility or other legal incapacity or exemption, or to unawareness of the criminal nature of the conduct solicited or of the defendant's criminal purpose or

¹ See Penal Law § 15.05(1). If necessary, an expanded definition of "intent" is available in the section on Instructions of General Applicability under Culpable Mental States.
to other factors precluding the mental state required for the commission of the crime in question. In other words, a defendant may be convicted of solicitation even though the person solicited could not be guilty of (specify the crime solicited).

In order for you to find the defendant guilty of this crime, the People are required to prove, from all the evidence in the case, beyond a reasonable doubt, both of the following two elements:

1. That on or about (date), in the County of (county), the defendant, (defendant's name), solicited, requested, commanded, importuned, or otherwise attempted to cause another person, namely (specify), to engage in conduct constituting a felony, namely (specify); and

2. That the defendant did so with the intent that (specify) engage in that conduct.

Therefore, if you find that the People have proven beyond a reasonable doubt both of those elements, you must find the defendant guilty of the crime of Criminal Solicitation in the Fourth Degree as charged in the _____ count.

On the other hand, if you find that the People have not proven beyond a reasonable doubt either one or both of those elements, you must find the defendant not guilty of the crime of Criminal Solicitation in the Fourth Degree as charged in the _____ count.

__________________________

2 Penal Law § 100.15.
CRIMINAL SOLICITATION
FIFTH DEGREE
(Violation)
PENAL LAW 100.00
(Committed on or after Sept. 1, 1978)

The _____ count is Criminal Solicitation in the Fifth Degree.

Under our law, a person is guilty of Criminal Solicitation in the Fifth Degree when, with intent that another person engage in conduct constituting a crime, he or she solicits, requests, commands, importunes or otherwise attempts to cause such other person to engage in such conduct.

The term "intent" used in this definition has its own special meaning in our law. I will now give you the meaning of that term.

INTENT means conscious objective or purpose.¹ Thus, a person acts with the intent that another person engage in conduct constituting a crime when his or her conscious objective or purpose is that such other person engage in such conduct.

Under our law, (specify the solicited crime) is a crime. A person is guilty of (specify the solicited crime), when (read the applicable portion of the statutory definition of the solicited crime).

Under our law, it is no defense to a prosecution for criminal solicitation that the person solicited could not be guilty of the crime solicited owing to criminal irresponsibility or other legal incapacity or exemption, or to unawareness of the criminal nature of the conduct solicited or of the defendant's criminal purpose or to other factors precluding the mental state required for the

1 See Penal Law § 15.05(1). If necessary, an expanded definition of "intent" is available in the section on Instructions of General Applicability under Culpable Mental States.
commission of the crime in question. In other words, a defendant may be convicted of solicitation even though the person solicited could not be guilty of (specify the crime solicited).

In order for you to find the defendant guilty of this offense, the People are required to prove, from all the evidence in the case, beyond a reasonable doubt, both of the following two elements:

1. That on or about ___(date)___, in the County of ___(county)___, the defendant, ___(defendant's name)___, solicited, requested, commanded, importuned, or otherwise attempted to cause another person, namely ___(specify)___, to engage in conduct constituting a crime, namely ___(specify)___; and

2. That the defendant did so with ___(specify)___ engage in that conduct.

Therefore, if you find that the People have proven beyond a reasonable doubt both of those elements, you must find the defendant guilty of the crime of Criminal Solicitation in the Fifth Degree as charged in the ______ count.

On the other hand, if you find that the People have not proven beyond a reasonable doubt either one or both of those elements, you must find the defendant not guilty of the crime of Criminal Solicitation in the Fifth Degree as charged in the ______ count.

2 Penal Law § 100.15.
OFFERING A FALSE INSTRUMENT FOR FILING
FIRST DEGREE
(E felony)
PENAL LAW 175.35 (1)
(Committed on or after Nov. 1, 1998)¹

The ______ count is Offering a False Instrument For Filing in the First Degree.

Under our law, a person is guilty of offering a false instrument for filing in the first degree when, knowing that a written instrument contains a false statement or false information, and with intent to defraud the state or any political subdivision, public authority or public benefit corporation of the state, he OR SHE offers or presents it to a public office, public servant, public authority or public benefit corporation with the knowledge or belief that it will be filed with, registered or recorded in or otherwise become a part of the records of such public office, public servant, public authority or public benefit corporation.

Some of the terms used in this definition have their own special meaning in our law. I will now give you the meaning of the following terms: "written instrument," and "intent," "public servant."

WRITTEN INSTRUMENT means any instrument or article, including computer data or a computer program, containing written or printed matter or the equivalent thereof, used for the purpose of reciting, embodying, conveying or recording information, or constituting a symbol or evidence of value, right,

¹ Effective November 1, 2014 (L 2013, ch 490), Penal Law § 175.35 was amended by adding a subdivision (2) and designating the existing crime, which remains unchanged except for the addition of gender-neutral language, as subdivision (1).
privilege or identification, which is capable of being used to the advantage or disadvantage of some person.\textsuperscript{2}

INTENT means conscious objective or purpose. Thus, a person acts with intent to defraud the state [or any political subdivision, public authority or public benefit corporation of the state], when that person's conscious objective or purpose is to defraud the state [or any political subdivision, public authority or public benefit corporation of the state].\textsuperscript{3}

PUBLIC SERVANT means any public officer or employee of the state or of any political subdivision thereof or of any governmental instrumentality within the state, or any person exercising the functions of any such public officer or employee. [The term public servant includes a person who has been elected or designated to become a public servant.]

In order for you to find the defendant guilty of this crime, the People are required to prove, from all of the evidence in the case, beyond a reasonable doubt, each of the following five elements:

1. That on or about (date), in the county of (County), the defendant, (defendant's name), offered or presented a written instrument to a public office, or public servant, [or public authority or public benefit corporation];

2. The defendant did so with the knowledge or belief that it would be filed with, registered, or recorded in, or otherwise become a part of the records of such public office, or public servant, [or public authority or public benefit corporation];

\textsuperscript{2} See Penal Law § 175.00 (3).

\textsuperscript{3} See Penal Law § 15.05 (1).
3. That the written instrument contained a false statement or false information;

4. That the defendant knew that the written instrument contained a false statement or false information; and

5. That the defendant offered or presented the written instrument with intent to defraud the state or any political subdivision, [or public authority or public benefit corporation] of the state.

Therefore, if you find that the People have proven beyond a reasonable doubt each of those elements, you must find the defendant guilty of the crime of Offering a False Instrument For Filing in the First Degree as charged in the ______ count.

On the other hand, if you find that the People have not proven beyond a reasonable doubt any one or more of those elements, you must find the defendant not guilty of the crime of Offering a False Instrument For Filing in the First Degree as charged in the ______ count.
OFFERING A FALSE INSTRUMENT FOR FILING
IN THE SECOND DEGREE
(A misdemeanor)
PENAL LAW 175.30
(Committed on or after September 1, 1967)

The ______ count is Offering a False Instrument For Filing in the Second Degree.

Under our law, a person is guilty of offering a false instrument for filing in the second degree when, knowing that a written instrument contains a false statement or false information, he or she offers or presents it to a public office or public servant with the knowledge or belief that it will be filed with, registered or recorded in or otherwise become a part of the records of such public office or public servant.

Some of the terms used in this definition have their own special meaning in our law. I will now give you the meaning of the following terms: "written instrument," and "public servant."

WRITTEN INSTRUMENT means any instrument or article, including computer data or a computer program, containing written or printed matter or the equivalent thereof, used for the purpose of reciting, embodying, conveying or recording information, or constituting a symbol or evidence of value, right, privilege or identification, which is capable of being used to the advantage or disadvantage of some person.¹

PUBLIC SERVANT means any public officer or employee of the state or of any political subdivision thereof or of any governmental instrumentality within the state, or any person exercising the functions of any such public officer or employee. [The term public servant includes a person who has been elected or designated to become a public servant.]²

¹ Penal Law § 175.00(3).
² See Penal Law § 10.00(15)
In order for you to find the defendant guilty of this crime, the People are required to prove, from all of the evidence in the case, beyond a reasonable doubt, each of the following four elements:

1. That on or about (date), in the county of (county), the defendant, (defendant's name), offered or presented a written instrument to a public office or public servant;

2. That the defendant did so with the knowledge or belief that it would be filed with, registered, or recorded in, or otherwise become a part of the records of that public office or public servant;

3. That the written instrument contained a false statement or false information; and

4. That the defendant knew that the written instrument contained a false statement or false information.

Therefore, if you find that the People have proven beyond a reasonable doubt each of those elements, you must find the defendant guilty of the crime of Offering a False Instrument for Filing in the Second Degree, as charged in the _____ count.

On the other hand, if you find that the People have not proven beyond a reasonable doubt any one or more of those elements, you must find the defendant not guilty of the crime of Offering a False Instrument for Filing in the Second Degree, as charged in the _____ count.
FALSIFYING BUSINESS RECORDS
FIRST DEGREE
(E felony)
PENAL LAW 175.10
(Committed on or after November 1, 1986)

The ______ count is Falsifying Business Records in the First Degree.

Under our law, a person is guilty of falsifying business records in the first degree when, with intent to defraud that includes an intent to commit another crime or to aid or conceal the commission thereof, that person:

Select appropriate alternative:
makes or causes a false entry in the business records of an enterprise; or

alters, erases, obliterator, deletes, removes or destroys a true entry in the business records of an enterprise; or

omits to make a true entry in the business records of an enterprise in violation of a duty to do so which he or she knows to be imposed upon him or her by law or by the nature of his or her position; or

prevents the making of a true entry or causes the omission thereof in the business records of an enterprise.¹

Some of the terms used in this definition have their own special meaning in our law. I will now give you the meaning of the following terms: "enterprise," "business record," "intent."

¹ Penal Law § 175.10 reads: "A person is guilty of falsifying business records in the first degree when he commits the crime of falsifying business records in the second degree, and when his intent to defraud includes an intent to commit another crime or to aid or conceal the commission thereof." The charge substitutes the language of falsifying business records in the second degree in the appropriate place.
ENTERPRISE means any entity of one or more persons, corporate or otherwise, public or private, engaged in business, commercial, professional, industrial, eleemosynary, social, political or governmental activity.  

BUSINESS RECORD means any writing or article, including computer data or a computer program, kept or maintained by an enterprise for the purpose of evidencing or reflecting its condition or activity.

INTENT means conscious objective or purpose. Thus, a person acts with intent to defraud when his or her conscious objective or purpose is to do so.

In order for you to find the defendant guilty of this crime, the People are required to prove, from all of the evidence in the case, beyond a reasonable doubt, each of the following two elements:

1. That on or about (date), in the county of (county), the defendant, (defendant's name),

   Select appropriate alternative:
   made or caused a false entry in the business records of an enterprise; or

   altered, erased, obliterated, deleted, removed or destroyed a true entry in the business records of an enterprise; or

   omitted to make a true entry in the business records of an enterprise in violation of a duty to do so which the

---

2 Penal Law § 175.00(1).

3 Penal Law § 175.00(2). "Computer data or a computer program" was added effective November 1, 1986.

4 Penal Law § 15.05(1).
defendant knew to be imposed upon him/her by law or by the nature of his/her position; or

prevented the making of a true entry or caused the omission thereof in the business records of an enterprise; and,

2. That the defendant did so with intent to defraud that included an intent to commit another crime or to aid or conceal the commission thereof.

[Note: If the affirmative defense does not apply, conclude as follows:

Therefore, if you find that the People have proven beyond a reasonable doubt both of those elements, you must find the defendant guilty of the crime of Falsifying Business Records in the First Degree as charged in the _____ count.

On the other hand, if you find that the People have not proven beyond a reasonable doubt either one or both of those elements, you must find the defendant not guilty of the crime of Falsifying Business Records in the First Degree as charged in the _____ count.]

[NOTE: If the affirmative defense does apply, continue as follows:

If you find that the People have not proven beyond a reasonable doubt either one or both of those elements, you must find the defendant not guilty of Falsifying Business Records in the First Degree as charged in _____ count.

On the other hand, if you find that the People have proven beyond a reasonable doubt both of the elements, you must consider an affirmative defense the defendant has raised. Remember, if you have already found the defendant not guilty of Falsifying Business Records in the First Degree, you will not consider the affirmative defense.
Under our law, it is an affirmative defense to this charge of Falsifying Business Records in the First Degree that the defendant, at the time he/she engaged in the conduct constituting the offense, was a clerk, bookkeeper or other employee who, without personal benefit, merely executed the orders of his/her employer or of a superior officer or employee generally authorized to direct his/her activities.

Under our law, the defendant has the burden of proving an affirmative defense by a preponderance of the evidence.

In determining whether the defendant has proven the affirmative defense by a preponderance of the evidence, you may consider evidence introduced by the People or by the defendant.

A preponderance of the evidence means the greater part of the believable and reliable evidence, not in terms of the number of witnesses or the length of time taken to present the evidence, but in terms of its quality and the weight and convincing effect it has. For the affirmative defense to be proved by a preponderance of the evidence, the evidence that supports the affirmative defense must be of such convincing quality as to outweigh any evidence to the contrary.

Therefore, if you find that the defendant has not proven the affirmative defense by a preponderance of the evidence, then, based upon your initial determination that the People had proven beyond a reasonable doubt both of the elements of Falsifying Business Records in the First Degree, you must find the defendant guilty of that crime as charge in the _____ count.

On the other hand, if you find that the defendant has proven the affirmative defense by a preponderance of the evidence, then you must find the defendant not guilty of Falsifying Business Records in the First Degree as charged in the _____ count.]
FALSIFYING BUSINESS RECORDS
SECOND DEGREE
(A misdemeanor)
PENAL LAW 175.05
(Committed on or after November 1, 1986)

The ______ count is Falsifying Business Records in the Second Degree.

Under our law, a person is guilty of falsifying business records in the second degree when, with intent to defraud, he or she:

Select appropriate alternative:

makes or causes a false entry in the business records of an enterprise; or

alters, erases, obliterates, deletes, removes or destroys a true entry in the business records of an enterprise; or

omits to make a true entry in the business records of an enterprise in violation of a duty to do so which he or she knows to be imposed upon him or her by law or by the nature of his or her position; or

prevents the making of a true entry or causes the omission thereof in the business records of an enterprise.

Some of the terms used in this definition have their own special meaning in our law. I will now give you the meaning of the following terms: "enterprise," "business record," "intent."

ENTERPRISE means any entity of one or more persons, corporate or otherwise, public or private, engaged in business, commercial, professional, industrial, eleemosynary, social, political
BUSINESS RECORD means any writing or article, including computer data or a computer program, kept or maintained by an enterprise for the purpose of evidencing or reflecting its condition or activity.  

INTENT means conscious objective or purpose. Thus a person acts with intent to defraud when his or her conscious objective or purpose is to do so.

In order for you to find the defendant guilty of this crime, the People are required to prove, from all of the evidence in the case, beyond a reasonable doubt, each of the following two elements:

1. That on or about (date), in the county of (county), the defendant, (defendant's name), made or caused a false entry in the business records of an enterprise; or

   altered, erased, obliterated, deleted, removed or destroyed a true entry in the business records of an enterprise; or

   omitted to make a true entry in the business records of an enterprise in violation of a duty to do so which the defendant knew to be imposed upon him/her by law or by the nature of his/her position; or

   prevented the making of a true entry or caused the

---

1 Penal Law § 175.00(1).
2 Penal Law § 175.00(2).
3 Penal Law § 15.05(1).
omission thereof in the business records of an enterprise; and,

2. That the defendant did so with intent to defraud.

[Note: If the affirmative defense does not apply, conclude as follows:

Therefore, if you find that the People have proven beyond a reasonable doubt both of those elements, you must find the defendant guilty of the crime of Falsifying Business Records in the Second Degree as charged in the _____ count.

On the other hand, if you find that the People have not proven beyond a reasonable doubt either one or both of those elements, you must find the defendant not guilty of Falsifying Business Records in the Second Degree as charged in the _____ count.]

[NOTE: If the affirmative defense does apply, continue as follows:

If you find that the People have not proven beyond a reasonable doubt either one or both of those elements, you must find the defendant not guilty of Falsifying Business Records in the Second Degree as charged in _____ count.

On the other hand, if you find that the People have proven beyond a reasonable doubt both of the elements, you must consider an affirmative defense the defendant has raised. Remember, if you have already found the defendant not guilty of Falsifying Business Records in the Second Degree, you will not consider the affirmative defense.

Under our law, it is an affirmative defense to this charge of Falsifying Business Records in the Second Degree that the defendant, at the time he/she engaged in the conduct constituting the offense, was a clerk, bookkeeper or other employee who, without personal benefit, merely executed the orders of his/her employer or of a superior officer or employee generally authorized
to direct his/her activities.

Under our law, the defendant has the burden of proving an affirmative defense by a preponderance of the evidence.

In determining whether the defendant has proven the affirmative defense by a preponderance of the evidence, you may consider evidence introduced by the People or by the defendant.

A preponderance of the evidence means the greater part of the believable and reliable evidence, not in terms of the number of witnesses or the length of time taken to present the evidence, but in terms of its quality and the weight and convincing effect it has. For the affirmative defense to be proved by a preponderance of the evidence, the evidence that supports the affirmative defense must be of such convincing quality as to outweigh any evidence to the contrary.

Therefore, if you find that the defendant has not proven the affirmative defense by a preponderance of the evidence, then, based upon your initial determination that the People had proven beyond a reasonable the elements of Falsifying Business Records in the Second Degree, you must find the defendant guilty of that crime as charge in the _____ count.

On the other hand, if you find that the defendant has proven the affirmative defense by a preponderance of the evidence, then you must find the defendant not guilty of Falsifying Business Records in the Second Degree as charged in the _____ count.]
CRIMINAL FACILITATION
FOURTH DEGREE
(A Misdemeanor)
(Facilitation of a felony)
PENAL LAW 115.00 (1)
(Committed on or after Sept. 1, 1978)

The ______ count is Criminal Facilitation in the Fourth Degree.

Under our law, a person is guilty of Criminal Facilitation in the Fourth Degree when, believing it probable that he or she is rendering aid to a person who intends to commit a crime, he or she engages in conduct\(^1\) which provides such person with means or opportunity for the commission thereof and which in fact aids such person to commit a felony.

Some of the terms used in this definition have their own special meaning in our law. I will now give you the meaning of the following terms: "intends" and "crime."

\(^1\) In 2013, Penal Law § 115.20 was added, stating:
"For purposes of [Penal Law article 115], such conduct shall include, but not be limited to, making available, selling, exchanging, giving or disposing of a community gun, which in fact, aids a person to commit a crime. 'Community gun' shall mean a firearm that is actually shared, made available, sold, exchanged, given or disposed of among or between two or more persons, at least one of whom is not authorized pursuant to law to possess such firearm. 'Dispose of' shall have the same meaning as that term is defined in section 265.00 of this chapter. 'Share' and 'make available' shall, in the case of a firearm, be construed to include knowingly placing such firearm at a location accessible and known to one or more other persons."

If a "community gun" is in issue, the trial court may, to the extent it deems appropriate, incorporate some or all of the language of that statute in this charge. Whether that statute only defines "conduct" and the remaining elements, particularly the culpable mental state, must be proven, or whether that statute defines a crime of "criminal facilitation" without the culpable mental state element remains to be determined.
INTENT means conscious objective or purpose. Thus, a person INTENDS to commit a crime when that person's conscious objective or purpose is to commit a crime.

Under our law, a CRIME is defined to include a misdemeanor or a felony. A person commits the felony of (specify the committed felony) when that person (read the applicable portion of the statutory definition of the committed felony).

Under our law, it is no defense to a prosecution for criminal facilitation that the defendant is not guilty of the felony which he/she facilitated because he/she did not act with the intent or other culpable mental state required for the commission thereof.

[NOTE: Add if appropriate: Under our law, it is no defense to a prosecution for criminal facilitation that the person facilitated was not guilty of the underlying felony owing to criminal irresponsibility or legal incapacity or exemption, or to unawareness of the criminal nature of the conduct in question or to other factors precluding the mental state required for the commission of such felony.]

[NOTE: Add if appropriate: Under our law, it is no defense to a prosecution for criminal

________________________________________

2 See Penal Law § 15.05 (1). If necessary, an expanded definition of “intent” is available in the section on Instructions of General Applicability under Culpable Mental States.

3 See Penal Law § 10.00 (6).

4 Where the defendant believed it probable that he or she was rendering aid to a person who intended to commit a particular crime, and that crime differs from the felony actually committed, the court should charge the applicable portions of the statutory definitions of both crimes.

5 See Penal Law § 115.10 (3).

6 See Penal Law § 115.10 (1).
facilitation that the person facilitated has not been prosecuted for or convicted of the underlying felony (or has previously been acquitted of the underlying felony).[7]

[NOTE: Add if appropriate:
The defendant may not be convicted of criminal facilitation in the fourth degree under this count upon the testimony of a person who has committed the felony charged to have been facilitated unless such testimony is corroborated by such other evidence as tends to connect the defendant with such facilitation.[8]

In order for you to find the defendant guilty of this crime, the People are required to prove, from all of the evidence in the case, beyond a reasonable doubt, each of the following three elements:

1. That on or about ____ (date) ____, in the county of (County), the defendant, (defendant's name), engaged in conduct which provided (specify person facilitated) with means or opportunity to commit a crime[9];

2. That the defendant did so believing it probable both: that (specify person facilitated) intended to commit such crime, and that he/she, the defendant, was rendering aid to (specify person facilitated) to do so; and

3. That the defendant's conduct in fact aided (specify person facilitated) to commit the felony of (specify the facilitated felony).


[9] If the indictment or bill of particulars alleges a particular crime, specify that crime in the first element.
Therefore, if you find that the People have proven beyond a reasonable doubt each of those elements, you must find the defendant guilty of the crime of Criminal Facilitation in the Fourth Degree as charged in the _____ count.

On the other hand, if you find that the People have not proven beyond a reasonable doubt any one or more of those elements, you must find the defendant not guilty of the crime of Criminal Facilitation in the Fourth Degree as charged in the _____ count.
CONSPIRACY
FIFTH DEGREE
(A Misdemeanor)
(Conspiracy to commit felony)
PENAL LAW 105.05(1)
(Committed on or after Sept. 1, 1978)

The _____ count is Conspiracy in the Fifth Degree.¹

Under our law, a person is guilty of Conspiracy in the Fifth Degree when, with intent that conduct constituting a felony be performed, he or she agrees with one or more persons to engage in or cause the performance of such conduct.

The term "intent" used in this definition has its own special meaning in our law. I will now give you the meaning of that term.

INTENT means conscious objective or purpose.² Thus, a person acts with the intent that conduct constituting a felony be performed when his or her conscious objective or purpose is that such conduct be performed.

Under our law, (specify the object felony) is a felony. A person is guilty of (specify the object felony), when (read the applicable portion of the statutory definition of the object felony).

Under our law, the People must also prove that one of the conspirators committed an overt act in furtherance of the

¹This charge contemplates a single integrated conspiracy. Whenever the possibility of more than one conspiracy is supported by a reasonable view of the evidence, the jury must be charged in accordance with the law as set forth in People v. Leisner, 73 N.Y.2d 140 (1989).

²See Penal Law § 15.05(1). If necessary, an expanded definition of “intent” is available in the section on Instructions of General Applicability under Culpable Mental States.
conspiracy. The agreement to engage in or cause the performance of a crime is not itself an overt act. The overt act must be an independent act that tends to carry out the conspiracy. The overt act can be, but need not be, the commission of the crime that was the object of the conspiracy.

In this case, the alleged overt act[s] is [are]: *(specify).*

*Note: Add when and to the extent appropriate:*

Under our law, it is no defense to a prosecution for conspiracy that, owing to criminal irresponsibility or other legal incapacity or exemption, or to unawareness of the criminal nature of the agreement or the object conduct or of the defendant's criminal purpose or to other factors precluding the mental state required for the commission of conspiracy or the object crime, one or more of the defendant's co-conspirators could not be guilty of conspiracy or the object crime.

In other words, a defendant may be convicted of conspiracy even though one or more or all of the other parties to the agreement are not guilty of conspiracy or *(specify the object crime).*

In order for you to find the defendant guilty of this crime, the People are required to prove, from all the evidence in the case,

---

3 See Penal Law § 105.20.


5 Penal Law § 105.30.

6 See People v. Berkowitz, 50 N.Y.2d 333 (1980). In an appropriate case, the Court may add the reason one or more of the parties to the agreement is not liable by charging for example, "because that party is a police officer or an agent of a police officer pretending to agree to engage in or cause the performance of the *(specify object crime)*"; or, "because that party is under sixteen years of age."
beyond a reasonable doubt, each of the following three elements:

1. That on or about ____(date)____, in the County of (county), the defendant, (defendant's name), agreed with one or more persons to engage in or cause the performance of conduct constituting the felony of (specify object felony);

2. That the defendant did so with the intent that such conduct be performed; and

3. That the defendant, or one of the persons with whom he/she agreed to engage in or cause the performance of such conduct, committed [the] [at least one] alleged overt act in furtherance of the conspiracy.

Therefore, if you find that the People have proven beyond a reasonable doubt each of those elements, you must find the defendant guilty of the crime of Conspiracy in the Fifth Degree as charged in the _____ count.

On the other hand, if you find that the People have not proven beyond a reasonable doubt any one or more of those elements, you must find the defendant not guilty of the crime of Conspiracy in the Fifth Degree as charged in the _____ count.

---

7If venue depends upon the place of the commission of an overt act rather than the situs of the agreement, refer to the county in the third element rather than in the first element. See Penal Law § 105.25(1).
CONSPIRACY
SIXTH DEGREE
(B Misdemeanor)
PENAL LAW 105.00
(Committed on or after Sept. 1, 1978)

The _____ count is Conspiracy in the Sixth Degree.¹

Under our law, a person is guilty of Conspiracy in the Sixth Degree when, with intent that conduct constituting a crime be performed, he or she agrees with one or more persons to engage in or cause the performance of such conduct.

The term "intent" used in this definition has its own special meaning in our law. I will now give you the meaning of that term.

INTENT means conscious objective or purpose.² Thus, a person acts with the intent that conduct constituting a crime be performed when his or her conscious objective or purpose is that such conduct be performed.

Under our law, (specify the object crime) is a crime. A person is guilty of (specify the object crime), when (read the applicable portion of the statutory definition of the object crime).

Under our law, the People must also prove that one of the conspirators committed an overt act in furtherance of the conspiracy.³ The agreement to engage in or cause the

¹This charge contemplates a single integrated conspiracy. Whenever the possibility of more than one conspiracy is supported by a reasonable view of the evidence, the jury must be charged in accordance with the law as set forth in People v. Leisner, 73 N.Y.2d 140 (1989).

² See Penal Law § 15.05(1). If necessary, an expanded definition of “intent” is available in the section on Instructions of General Applicability under Culpable Mental States.

³ See Penal Law § 105.20.
performance of a crime is not itself an overt act. The overt act must be an independent act that tends to carry out the conspiracy. The overt act can be, but need not be, the commission of the crime that was the object of the conspiracy.\(^4\)

In this case, the alleged overt act[s] is [are]: \(\textit{specify}\).

\[\text{Note: Add when and to the extent appropriate:}\]

Under our law, it is no defense to a prosecution for conspiracy that, owing to criminal irresponsibility or other legal incapacity or exemption, or to unawareness of the criminal nature of the agreement or the object conduct or of the defendant's criminal purpose or to other factors precluding the mental state required for the commission of conspiracy or the object crime, one or more of the defendant's co-conspirators could not be guilty of conspiracy or the object crime.\(^5\)

In other words, a defendant may be convicted of conspiracy even though one or more of all of the other parties to the agreement are not guilty of conspiracy or \(\textit{specify the object crime}\).\(^6\)

In order for you to find the defendant guilty of this crime, the People are required to prove, from all the evidence in the case, beyond a reasonable doubt, each of the following three elements:

1. That on or about \((\text{date})\), in the County of __


\(^5\) Penal Law § 105.30.

\(^6\) See People v. Berkowitz, 50 N.Y.2d 333 (1980). In an appropriate case, the Court may add the reason one or more of the parties to the agreement is not liable by charging for example, "because that party is a police officer or an agent of a police officer pretending to agree to engage in or cause the performance of the \(\textit{specify object crime}\)"; or, "because that party is under sixteen years of age."
(county) ____, the defendant, (defendant's name), agreed with one or more persons to engage in or cause the performance of conduct constituting the crime of (specify object crime);

2. That the defendant did so with the intent that such conduct be performed; and

3. That the defendant, or one of the persons with whom he/she agreed to engage in or cause the performance of such conduct, committed [the] [at least one] alleged overt act in furtherance of the conspiracy.

Therefore, if you find that the People have proven beyond a reasonable doubt each of those elements, you must find the defendant guilty of the crime of Conspiracy in the Sixth Degree as charged in the _____ count.

On the other hand, if you find that the People have not proven beyond a reasonable doubt any one or more of those elements, you must find the defendant not guilty of the crime of Conspiracy in the Sixth Degree as charged in the _____ count.

7 If venue depends upon the place of the commission of an overt act rather than the situs of the agreement, refer to the county in the third element rather than in the first element. See Penal Law § 105.25(1).
ATTEMPT TO COMMIT A CRIME
PENAL LAW § 110.00

The _________ count is attempt to commit the crime of _________.
(attempted crime)

I shall instruct you first on the definition of the crime of _________. Then I shall define for you an attempt to commit a crime. Finally, I shall put both definitions together and list for you the elements of attempt to commit the crime of _________.
(attempted crime)

_________________

[NOTE: Here read statutory definition of crime and any defined terms as set forth in CJI for that crime.]

_________________

Under our law, a person is guilty of an attempt to commit a crime when, with intent to commit a crime, he or she engages in conduct which tends to effect the commission of such crime.¹

Some of the terms used in this definition have their own special meaning in our law. I will now give you the meaning of the following terms: "intent" and "tends to effect."

INTENT means a conscious objective or purpose. Thus, a person acts with intent to commit a crime when his or her conscious objective or purpose is to commit that crime.²

Conduct which TENDS TO EFFECT the commission of a crime means conduct which comes dangerously close or very near to the completion of the intended crime.

_________________

¹ See Penal Law §110.00.

² See Penal Law § 15.05(1). If necessary, an expanded definition of “intent” is available in the section on Instructions of General Applicability under Culpable Mental States.
If a person intends to commit a crime and engages in conduct which carries his or her purpose forward within dangerous proximity to the completion of the intended crime, he or she is guilty of an attempt to commit that crime. It does not matter that the intended crime was not actually completed.

The person's conduct must be directed toward the accomplishment of the intended crime. It must go beyond planning and mere preparation, but it need not be the last act necessary to effect the actual commission of the intended crime. Rather, the conduct involved must go far enough that it comes dangerously close or very near to the completion of the intended crime.³

[NOTE: Add where factual or legal impossibility is an issue:
It is no defense in a prosecution for an attempt to commit a crime that the intended crime was, under the circumstances, factually or legally impossible to commit, if such crime could have been committed had the circumstances been as the defendant believed them to be.]⁴


⁴ See Penal Law § 110.10.
NOTE: Select one of the following two conclusions:  

\[\text{If intent applies to every element of the crime, conclude as follows:}\]

In order for you to find the defendant guilty of an attempt to commit the crime of \((\text{specify})\), the People are required to prove, from all the evidence in the case, beyond a reasonable doubt, both of the following two elements:

1. That on or about \((\text{date})\), in the county of \((\text{county})\), the defendant, \((\text{name of defendant})\), intended to commit the crime of \((\text{specify})\); and

2. That the defendant engaged in conduct which tended to effect the commission of that crime.

Therefore, if you find that the People have proven beyond a reasonable doubt both of those elements, you must find the defendant guilty of the crime of attempt to commit the crime of \((\text{specify})\) under the _____ count.

On the other hand, if you find that the People have not proven beyond a reasonable doubt either one or both of those elements, you must find the defendant not guilty of the crime of attempt to commit the crime of \((\text{specify})\) under the _____ count.

---

5 \text{People v. Miller, 87 NY2d 211 (1995), held that a defendant could be guilty of an attempt to commit Robbery in the First Degree, under PL §§ 20.00 and 160.15(1), provided he intended to forcibly steal property, even though he did not intend the serious physical injury to a non-participant which resulted; intent applied only to the "core" crime of robbery, not the non-intentional "aggravating element"). When intent applies to every element of the attempted crime, use or adapt the first alternative in the text. In the Miller situation, where a defendant may be guilty of an attempt although his intent does not encompass every element of the crime, use or adapt the second alternative.}
[If there are some elements of the attempted crime to which
intent does not apply, conclude as follows:]

In order for you to find the defendant guilty of an attempt to
commit the crime of (specify), the People are required to prove,
from all the evidence in the case, beyond a reasonable doubt,
each of the following three elements:

1. That on or about (date), in the county of (county), the
defendant, (name of defendant), intended to commit the
crime of (specify core crime);

2. That the defendant engaged in conduct which tended
to effect the commission of that crime; and

3. That (specify strict liability element which raises degree of
intended crime).  

Therefore, if you find that the People have proven beyond
a reasonable doubt each of those elements, you must find the
defendant guilty of the crime of attempt to commit the crime of (specify) under the ______ count.

On the other hand, if you find that the People have not
proven beyond a reasonable doubt any one or more of those
elements, you must find the defendant not guilty of the crime of

6 For example, for Attempted Robbery in the First Degree under Penal
Law §§ 20.00 and 160.15(1), the "core crime" in the first element would be
"robbery" and the third element would read:

3. That in the course of the attempted commission of the crime
[or of immediate flight therefrom], the defendant [or another
participant in the crime] caused serious physical injury to
(specify), and (specify) was not a participant in the robbery.
attempt to commit the crime of 
(specify) under the ________ count.
EVOLVING AML JOURNEY

BALANCING INTERNAL, EXTERNAL AND VIRTUAL WORKFORCES: AN EVOLVING ANTI-MONEY LAUNDERING OPERATING MODEL FOR 2020
Due to increased regulatory scrutiny and pressures, banks have invested heavily in Anti-Money Laundering (AML), adding headcount to both establish and maintain compliance. Many banks’ AML-related activities suffer from a high cost base, often as the result of an inefficient operating model.

This has led to “regulatory fatigue” among overworked staff. It has also created a bidding war for individuals with AML-related skills and experience.

Banks, facing continual pressure to increase margins and reduce operating costs, are exploring technological solutions, including Robotic Process Automation (RPA) and Artificial Intelligence (AI), as well as process-oriented approaches such as Managed Services.

New players in the financial services ecosystem, such as FinTech (financial technology) payments companies and new “online only” banks are even choosing to build “virtual” AML functions, outsourcing all or most of their operational AML processes.

These “point” solutions are helpful, and should be applied as part of an overarching AML Operating Model that can scale and innovate with changing technology. A comprehensive model can help financial institutions balance the competing challenges of regulatory compliance, flexibility and efficiency.
In determining where best to implement point solutions to help reduce cost and drive efficiency, banks should evaluate where they can derive the greatest benefit by reallocating resources with targeted skills.
CAPABILITY GROUPS IN THE AML OPERATING MODEL

Every financial institution should establish a Bank Secrecy Act (BSA) and AML operating model which can deliver the foundational capabilities to meet the “four pillars” of AML compliance,\(^1\), as listed below.

1. A system of internal controls for ongoing compliance.
2. Independent testing of BSA/AML compliance.
3. A specifically designated person or persons responsible for managing BSA/AML compliance (BSA/AML compliance officer).
4. Training for appropriate personnel.

As outlined in Figure 1, these capabilities fall into two major groupings:

1. **Core operational capabilities**, including Customer Due Diligence (CDD) at Onboarding and Refresh, Transaction Monitoring and Screening. These are passive capabilities which do not provide competitive differentiation, and scale with increasing transaction volumes and regulatory demands.

2. **Oversight capabilities**, including capabilities such as Risk Assessment, AML Training and Learning Development, Controls Testing, and Quality Assurance. Typically, these are higher complexity, active capabilities requiring an in-depth understanding of the bank’s customers, risk appetite and organization.

In determining where best to implement point solutions to help reduce cost and drive efficiency, banks should evaluate where they can derive the greatest benefit by reallocating resources with targeted skills. This necessitates taking a closer look at both core operational (passive) and at oversight (active) capabilities and deciding which capabilities to carry out in-house, which to automate, and which to outsource.
Figure 1. BSA/AML and Sanctions Compliance Program Functional Operating Model

ANTI-MONEY LAUNDERING COMPLIANCE OFFICER

AML OVERSIGHT AND CONTROL FUNCTIONS

- AML Risk Assessment
- AML Policy & Standards
- Regulatory Inventory & Change Management
- AML Compliance Advisory
- Analytics & Intelligence
- Training & Learning Development
- Staffing & Workforce Planning
- Quality Assurance & AML Compliance Testing

AML OPERATIONS FUNCTIONS

- CDD & Refresh
- Politically Exposed Persons (PEPs), Senior Political Figures (SPFs) & Adverse Media Screening
- Office of Foreign Assets Control (OFAC) & Sanctions Screening
- Transaction Monitoring
- Investigations
- Client Offboarding
- Internal Controls
- Reporting & Escalations

Source: Accenture, September 2017
Operational processes have been the focus of investment for banks in recent years.

Banks typically respond to AML-related Consent Orders or Matters Requiring Attention (MRAs) by adding staff to conduct transaction monitoring alert investigations, Know Your Customer (KYC) reviews for onboarding and refresh activities, and screening alert reviews, among other activities.

Although 50 percent of banks say they have added employees to keep up with KYC compliance over the past year, banks still indicate they do not have enough people with the right skills. In fact, 70 percent of respondents to a recent survey said they had to dedicate more time to KYC-related issues over the previous 12 months, diverting attention and resources from more strategic, revenue-related activities.

Core operational capabilities are characterized by high volume and low complexity, but they are often labor-intensive, requiring significant manual processing. These are typically “passive” functions that consume resources without providing a competitive advantage.

Rather than hiring or assigning employees for these functions, banks should use a combination of virtual and external workforce elements to create value in these areas. Experience has shown that the combination of RPA and managed services can help reduce internal operations headcount by up to 70%, providing an efficient, scalable and cost-effective solution for AML processes (see Figure 2).

A non-physical or virtual workforce, comprised of RPA and, to a growing extent, AI can automate low-value activities, increasing efficiency and reliability.

RPA and AI-based solutions can perform labor-intensive activities that do not rely upon human judgment (for example, gathering basic customer information like the customer’s correct registered address from third-party sources). According to an article by UiPath, Inc., companies implementing RPA solutions have reported cost reductions of 35 to 65 percent for onshore process operations and 10 to 30 percent for offshore delivery, with an investment recovery period as short as six to nine months.

For the remainder of core operational activities, banks should leverage an external workforce, using a third-party provider to perform these tasks via managed services. Managed services can provide an extended workforce to supervise and conduct activities characterized by low complexity and high volume, freeing the existing workforce to scale to more strategic tasks. External sourcing could provide significant benefits, including:
• The flexibility and/or scalability to address peaks and troughs in demand, with access to appropriate skills
• The transfer of the managerial burden of staffing and supervising day-to-day operations, as well as the application of HR requirements, to a third party
• Improvements in overall quality due to specialization and concentrated expertise
• Cost and efficiency savings realized through a variable cost structure, and using a managed services model for AML and/or KYC activities—these are reported to be in the 20 to 60 percent range⁵
• Increased capacity of the internal workforce to focus on more strategic, higher value-added activities

Banks then face the question of how to descale the remaining workforce, migrate and upskill talent to address oversight capabilities, and address their organizational culture to avoid attrition.

Figure 2. BSA/AML and Sanctions Program Opportunities for Transformation

Source: Accenture, September 2017
UPGRADING OVERSIGHT CAPABILITIES

In contrast with operational capabilities, oversight capabilities are active capabilities requiring a skilled workforce with specific knowledge of the bank’s organizational structure and risk appetite.

As seen in Figure 3, target skills for these resources can be grouped into performance drivers, functional competencies, and, to some degree, specialist skills for non-manual processing functions. Executives with oversight responsibilities over these resources require decision-making authority to perform their roles.

Oversight capabilities have not been an area of focus for banks’ AML compliance programs, with focus traditionally centered on evidence of compliance to regulatory change. In recent AML compliance audits, these functions have increasingly been cited as key areas for potential improvement, particularly in more robust training programs, closer traceability between policies and procedures, and in the assessment of risk.

Due to the complexity of these tasks driving the need for expertise and judgment, the internal workforce should play a key role in oversight activities. Coupled with the selective use of AI sub-components, such as Natural Language Generation to support policy documentation, virtual assistants to support AML compliance advisory activities, and Natural Language Processing to support regulatory change management, the Center of Excellence (CoE) approach is an innovative way to develop and transform strategic capabilities while reducing costs.

CoEs allow banks to meet regulatory requirements and provide independent testing for AML compliance programs; internal reviews of business controls for quality management; the performance of regular, robust risk assessments; and consistent, comprehensive AML training. Key benefits of this approach include:

- Robust AML capabilities to drive compliance
- Standardized processes across the enterprise, reducing the cost of compliance
- Clear career paths, improving morale and thus retention
- Improvements in overall quality due to specialization and concentrated skills

When building the AML operating model of the future, banks should rethink their operating models to consider what is handled in-house through scalable CoEs and existing workforce, what can be automated, and what can be sourced through managed services. This allows banks to have the right capabilities to drive compliance, without adding unnecessary headcount and cost in response to consent orders or MRAs.
Figure 3. Target Skills for Resources

**#1 – Performance Drivers**
Performance drivers are behavioral, management and leadership competencies that underpin high performance, rather than acceptable performance, in any role or function. A company-wide focus on these skills can help drive towards a high-performance organization.

**#2 – Functional Competencies**
Functional competencies are specific and key skills, knowledge and behaviors to be performed in specific areas of the organization. For example, within sales, one may require a detailed understanding of account management that may not be required in other functional areas.

**#3 – Specialist Skills**
Specialist skills are specific industry, process and/or technical solution skills related to the completion of particular roles. These skills help identify subject matter knowledge within business areas.

<table>
<thead>
<tr>
<th>Customer &amp; Client Centricity</th>
<th>Banking Industry Knowledge</th>
<th>Policy Definition &amp; Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performing Through our People</td>
<td>General Financial Crime Knowledge</td>
<td>Case Investigations &amp; Analysis</td>
</tr>
<tr>
<td>Managing Risk – Financial Crime, Reputation, etc.</td>
<td>Legislative &amp; Regulatory Environment</td>
<td>AML &amp; Economic Sanctions Specific Knowledge</td>
</tr>
<tr>
<td>Communicating for Impact</td>
<td>Account Planning, Development &amp; Management</td>
<td>Training Design, Development &amp; Delivery</td>
</tr>
<tr>
<td>Delivering Results and Operational Excellence</td>
<td>Negotiation</td>
<td>Policies, Standards &amp; Procedures</td>
</tr>
<tr>
<td>Leadership</td>
<td>Consulting &amp; Advisory Skills</td>
<td>Financial Services Products &amp; Services</td>
</tr>
<tr>
<td>Business Knowledge Acumen</td>
<td>Project, Program &amp; Delivery Management</td>
<td>Risk Advisory</td>
</tr>
<tr>
<td>Written &amp; Verbal Communication</td>
<td>Business Relationship Management</td>
<td>Compliance Testing</td>
</tr>
<tr>
<td>Developing Talent &amp; Skills</td>
<td>Productive &amp; Effective Working Practices</td>
<td>Systems, Technology Applications &amp; Tools</td>
</tr>
<tr>
<td></td>
<td>IT &amp; System Integration</td>
<td></td>
</tr>
</tbody>
</table>

Source: Accenture, September 2017
CHALLENGES IN TRANSFORMING THE AML OPERATING MODEL

Many banks may find that internal staff lack the skills needed for high value-added strategic activities. In addition, because of frequent technology changes and new regulations, internal staff should be able to adopt new skills quickly.

To take on new strategic roles, banks should also teach new skills to the internal workforce in a fast, effective manner.

When transforming their AML operating model, banks face a significant obstacle in identifying, developing and retaining a workforce with the skills to perform the appropriate tasks. This difficulty is compounded by the scarcity and high cost of talent. Rather than recruiting externally, banks should focus on sourcing internally, helping their workforce develop the skills needed to focus on higher value-added activities.

After leveraging RPA, AI and managed services to streamline core operational processes, banks can release talent to focus on oversight activities. Developing talent internally helps provide growth opportunities and new career paths (both important for increasing employee engagement) while reducing costs.

Cultural issues can also present a challenge. Banks should work to make it clear that the company culture supports employee growth and education. This can help reduce attrition caused by organizational change, or by the fear that roles and headcount are tied only to changing regulatory requirements.

Internal development of talent requires a robust talent management program with scalable roles, responsibilities, and clear career paths to give talent the right combination of skills for the new roles being created. The objective is to provide more interesting, enriching work as employees perform new tasks required by the regulatory environment.

A review of learning effectiveness, as illustrated in Figure 4, can support the revised talent framework. The purpose of the review is to:

- Identify needed new behaviors and leadership skills
- Determine proper employee proficiency levels
- Measure success against agreed-upon key performance indicators (KPIs)
- Increase employee engagement and exposure to new concepts
Another challenge to the implementation of an AML operating model is having a flexible and adaptive workforce. Employees engaged in oversight activities require different skills and the ability to make decisions. Evolved Operating Models push technology and outsourced resources to cover previously staffed roles, allowing employees formerly involved in operating activities the time and focus to obtain new skills. When properly trained, these employees can exercise judgment and elevate issues as circumstances dictate.

The return on investment in training and development is measured by the financial return on the reallocation of talent to increasingly complex roles. The bank should realize savings on recruitment costs, on reduced attrition, and on a shorter time to competency for new skills. The culture of opportunity and growth should make it easier to attract and retain top talent.

Figure 4. Measuring Learning Effectiveness

Learning Effectiveness and Impact

To be effective, learning programs should have a number of positive, measurable impacts

**POTENTIAL IMPACT AREAS**

- Gain new behaviors and leadership skills
- Employee proficiency levels
- Improvement in business performance (identified through success measures)
- Employee engagement
- Exposure and networking opportunities

**METRICS/DATA AVAILABLE**

1. Learning satisfaction
2. Maintain or increase performance ratings
3. Increase in number of self-initiated trainings
4. Employee retention
5. Improvement in success related metrics or KPIs

**POTENTIAL NEW WAYS TO MEASURE**

1. 1-5 Kirkpatrick Levels
2. Direct Impact of Learning
3. Indirect Impact of Learning
4. Increased utilization
5. Level 3 measures - feedback from supervisor on effectiveness or on proficiency (before and after)

Note: The Kirkpatrick model is a worldwide standard for evaluating the effectiveness of training. See: http://www.kirkpatrickpartners.com/Our-Philosophy/The-Kirkpatrick-Model

Source: Accenture, September 2017
CONCLUSION

Regulatory pressure related to AML issues is likely to continue and may increase. Financial institutions are encouraged to balance regulatory compliance requirements with demands for greater efficiency.

A blended and scalable AML operating model is essential for establishing and maintaining this balance.

This innovative approach to operating models also helps banks set out a clear strategy for the application of RPA, AI and managed services, helping improve ROI. It helps determine which capabilities can be assigned to third-party providers, which can be automated and which should be retained in-house.

To support this transformation, banks should consider a targeted talent development program to give their internal workforce the skills and competencies needed to perform increasingly complex assignments.

In our view, this approach to AML operating model transformation can provide banks with the flexibility and scalability to meet fluctuating regulatory demands. This should not be static in nature. New demands will arise and a properly designed model can align itself with other risk functions, such as operational risk and cyber risk, as the risk environment evolves. In addition to cost efficiency, banks can also realize quality gains through increased automation and improved training of individuals involved in oversight functions. In addition, the bank’s commitment to internal sourcing and training can create new opportunities for employees, reducing attrition and making it easier to develop talent internally.
ABOUT THE AUTHORS

Samantha Regan
Samantha is a Managing Director, and is the North America Lead for the Regulatory Remediation & Compliance Transformation group within Accenture’s Finance & Risk practice. Based in New York, she has 17 years of global experience working with C-suite executives and their businesses in compliance and regulatory initiatives.

Philippe Guiral
Philippe is a Senior Manager, Accenture Finance & Risk, based in New York. He leads Accenture’s North America Financial Crime Group, and has over 12 years of experience, defining capabilities and strategies to support clients in their financial crime prevention programs in both the UK and the US. Philippe specializes in delivering large-scale complex business and technology financial crime change programs to drive high performance.

Garikai Mparutsa
Garikai is Senior Manager, Accenture Finance & Risk. Based in New York, Garikai is an experienced financial crime consulting professional having worked with major retail banking and capital markets institutions in the UK, US, Europe and Asia. His recent focus has been on assessing the impact of new banking regulations on operating models, designing organizational structures to meet target end states, and defining strategic options to address idiosyncratic governance and control failures.

Cathy Dunne
Cathy is a Manager, Accenture Finance & Risk, based in New York. Cathy is an experienced consulting professional, having worked on key strategic and transformational initiatives for leading financial services organizations in both the US and Europe. Her recent focus has been on Anti-Money Laundering and Financial Crime, developing operating models, designing organizational structures and building AML capabilities to drive compliance for top global banks and leaders in the FinTech sector.

Rebecca Alberico
Rebecca is a Manager, Accenture Financial Services, based in Chicago. A member of the North America, Accenture Talent and Organization Performance offering group, she leads the Learning and Collaboration program for the Finance & Risk practice. Rebecca’s experience and focus are in the areas of training content design and development, skill-to-role curriculum solutions, and organizational change management focusing on Financial Crime and Regulatory Compliance.
To support this transformation, banks should consider a targeted talent development program to give their internal workforce the skills and competencies needed to perform increasingly complex assignments.
Evolving AML Journey

Leveraging Machine Learning within Anti-Money Laundering Transaction Monitoring
Artificial Intelligence (AI) and one of its key components, Machine Learning (ML) are innovative and disruptive technologies that are widely used within many industrial sectors, including life sciences, automotive, aerospace and defense.

However, despite numerous potential applications within the financial services sector, specifically within Anti-Money Laundering (AML), adoption of AI and ML has been relatively slow. This has been, in part, due to the following: (1) limited comprehension of the application of AI and ML within AML compliance programs; (2) the notion of ML being a “black box” where the inner workings are not clearly understood by regulators and compliance officers; and (3) the cautious approach taken by regulators requiring compliance officers to understand and validate how outcomes from AML models are arrived at.

Nevertheless, when coupled with hybrid models involving human resources supported by AI, AML solutions can be developed that provide significant benefits, including a reduction in compliance costs and improvements in the transaction monitoring process leading to greater overall efficiency.
AI is a field of computer science focused on the development of computers to carry out activities typically executed by humans, specifically activities requiring humans to take decisions and rely on their intelligence.

There are several component technologies within AI all with numerous applications. For example, Natural Language Processing (NLP), through which computers process human language, is used for translating payments in payment screening, processing mortgage applications and negative news screening (see Figure 1).

ML is a sub-field of AI where computers are able to learn when exposed to new data without being explicitly programed. The potential applications for this within suspicious activity monitoring and Transaction Monitoring (TM) are vast.

A common TM challenge is the generation of a vast number of alerts requiring costly operations teams to triage the alerts. With increasing customer numbers, and increasing numbers of transactions, TM alert volumes have increased significantly at financial institutions (FIs). This increase in alerts has resulted in an upsurge in the number of personnel required to triage and process them. However, in leveraging ML at the alert triage stage, alerts can potentially be suppressed, hibernated (set aside for later examination) or even, at some time in the future, closed automatically.

ML can teach computers to detect and recognize suspicious behavior and classify alerts following a risk-based approach as being of high, medium or lower risk. Applying rules to these alert classifications can facilitate hibernation and auto closure of alerts, allowing human resources to supervise machines that triage these alerts rather than reviewing alerts manually. This change is illustrated in Figure 2.

Machines can be taught to recognize, score, triage, enrich, close or hibernate alerts. This can help focus experienced human resources on complex problems while computers perform simpler tasks for them. By using AI across the entire TM process, alerts can be auto-triaged leveraging ML; they can be auto-enriched with account, transaction, and customer information from external and internal data sources leveraging intelligent automation and NLP; and narratives for Suspicious Activity Reports (SARs) can be auto-generated using Natural Language Generation (NLG). Institutions leveraging AI in this way can reduce dependencies on human operators to perform routine tasks, reduce the total time it takes to triage alerts, and allow personnel to focus on more valuable and complex activities.
Figure 1. Illustration of some AI Applications and Components

Other components include, Genetic Algorithms and Swarm Intelligence. This document largely focuses on ML for AML TM.

Figure 2. Introducing ML into AML TM Alert Triage

With the introduction of ML into AML TM alert triage, SAR conversion rates should improve from the current unacceptable rate of ~1% in the banking sector.
CHALLENGES TO IMPLEMENTING ML

Through Accenture’s work with global FIs we have identified a number of implementation challenges for financial services firms seeking to implement ML as part of AML TM solutions.

Figure 3. The Challenges to Implementing ML as part of a TM Solution

- **DQM and Profile Refresh**
- **Lack of a 360-degree View of the Customer**
- **Limited Knowledge of both Financial Services and ML**
- **Limited Regulatory Appetite**
- **Lack of Straightforward Processes**

Source: Accenture, September 2017
These challenges include poor data quality, low Know Your Customer (KYC) profile refresh rates, lack of a holistic view of the customer, limited knowledge of both financial services and ML, regulatory expectations and appetite, and lack of straightforward processes to follow for implementation.

1. **Data quality management and profile refresh.** Data Quality Management (DQM) is a required activity for all monitoring systems and analytics. It is not unique in any way to ML applications. Both static files, for example KYC files, and dynamic data held by FIs on their customers’ transactions have seen low completeness ratios in areas such as missing payment information and high error rates in recent years. Additionally, there is also a general lack of data traceability and data lineage.

Some FIs address data issues on an alert and/or profile basis when alerts are generated as false positives or noise. This method reduces reoccurrence of noise or false positives. However, others prefer large-scale, one-off data reconciliation/refresh exercises. During the last few years, many FIs have undertaken large and costly data remediation projects to improve data and have implemented frameworks to manage data quality. However, data quality remains an ongoing problem.

To the challenge of missing and outdated data, there is an opportunity to tie profile refreshes into sales and marketing exercises. Relationship managers can use profile refresh opportunities to reach out to their customers and identify cross-selling opportunities.

2. **Lack of a 360-degree view of the customer.** Another challenge in implementing ML-supported TM programs is the inability for FIs to build a 360-degree view of the customer. For example, financial services firms do not have the global freedom to share information about their customers to build a comprehensive network. Furthermore, FIs do not formally collaborate on AML as this is a cost. Building a 360-degree view would require collaboration across FIs and information agencies that does not exist today.

Currently, once FIs decide to file an SAR and submit it to the regulator, there is limited feedback and intelligence returned. In addition to sharing information securely between FIs and regulators, external (to KYC) data sets can be used in areas such as marketing data, which has rich datasets on customer behavior not generally used for AML behavior modeling and alert enrichment and/or triage. However, there have been some developments in recent years that are paving the way to alleviate this challenge of data sharing. Regulators are increasingly leaning toward data sharing between banks. Relevant regulations encouraging data sharing are US Patriot Act 314 a and 314 b and PSD2. The UK Treasury is also encouraging sharing of data via an Open Banking API/Open Banking Working Group. However, data ownership, medium (e.g. cloud) and the extent of this data sharing needs to be defined. It is a matter of time before large amounts of transactional data will become available on intrabank data clouds.
3. **Limited knowledge of both financial services and ML.** Another reason why ML has not been as widely applied within the financial services industry is that very few people are experts in both ML techniques and financial services. As a result, there have been fewer applications targeting financial services problems from start-ups and established vendors, limiting acceptance of ML within the financial services sector (especially for financial crime prevention).

4. **Limited regulatory appetite.** FIs have held back from implementing ML solutions because regulators expect models that can be clearly understood. They typically insist that all choices, limitations, and results be documented before such models are implemented. In the regulators’ view, the models should be designed in a way that allows for results to be reproduced given the same input data. This is not always possible with ML algorithms.

   Additionally, there is some evidence that large vendors are, in effect, acting as leading regulators. This is because some regulators recommend specific solutions for TM that are ineffective and generally need to be replaced by intelligent and adaptive solutions. These large players dominate the technology space and, consequently, there is only a narrow field of play for start-ups. Start-ups tend to need support from consultancies and other third parties that help banks with their evaluations and implementations.

5. **Lack of straightforward processes.** ML is a relatively new technology and there are few established, straightforward processes to follow to implement it. Without knowing what to look for, teaching systems to detect certain types of financial crime can be tricky. For example, how does one teach a system to recognize terrorist financing? There is a carousel process for fraud but nothing similar for terrorist financing (nothing, that is, other than name matching against terrorist lists). While some of these problems are better suited to unsupervised learning, model validators should be sure about the desired outcomes.
MODEL VALIDATION AND BLACK BOX TECHNIQUES FOR ML AML MODELS

Any statistical model chosen by an FI for TM needs to follow steps similar to those illustrated in Figure 4.

These steps are recommended by the Office of the Comptroller of the Currency (OCC) for model risk management.1 Extensive documentation is required for models selected and the regulators expect FIs to be able to re-create results and explain exactly how their models work.

The introduction of ML opens up numerous new techniques for TM, all constructed with mathematical equations. Some of these algorithms or techniques are simpler to understand than others. Simpler algorithms include decision trees while more complex algorithms may comprise neural networks.

Algorithms that are predictable, traceable, and simple to explain are “white box” techniques. On the other hand, more complex algorithms are known as “black boxes,” as the mathematical calculations underlying these techniques are far too dense and complex to be able to recreate results and provide rationale for the learned parameters (such as weighting). Figure 5 illustrates how model validation becomes more complicated as techniques move from “white box” to “black box.”

Currently, there is no straightforward method to validate complex or black box ML model choices for internal auditing and for external regulatory purposes. Black box ML techniques can be tested by adopting (and adapting) the Turing test, whereby human analysts are trained with the same samples as machines and an observer evaluates results to determine precision and recall. At the same time the observer needs to determine which results were produced by a human and which were produced by an ML system. This process could be undertaken as an interbank activity, possibly with the involvement of regulators.

However, just as current TM systems require their scenarios and segments to be updated, ML-based TM systems will also have to be updated periodically. This can be more complicated than standard TM system maintenance and ongoing testing is required. Realistically, such testing and updating should be consultancy or vendor driven as part of an ongoing maintenance contract. The slightest change in the type of data that once produced desired results can render the system unreliable.
Figure 4. Summary of Model Risk Management Guidance from the OCC

<table>
<thead>
<tr>
<th>CONCEPT SOUNDNESS</th>
<th>ONGOING MONITORING</th>
<th>OUTCOME ANALYSIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>· All model choices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Mathematical calculations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Key assumptions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Data, selection of inputs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Limitations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Benchmarking (precision, recall, harmonic mean)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· User feedback</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Limitations assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Time periods for testing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Sensitivity analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Back testing (actual vs. forecast)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Testing approaches</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Test data and outcomes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Supervisory Guidance on Model Risk Management, Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency

Figure 5. Complexity Scale for Model Validation of ML Algorithms

Source: Accenture, September 2017
HOW ACCENTURE CAN HELP

Accenture provides services to global FIs to implement both ML and robotic process automation (RPA) programs.

We have extensive capabilities in this area, including analytics and digital centres of excellence and subject matter specialists to:

- Identify and analyze business opportunities
- Assess the impact of possible solutions (such as updating procedure manuals versus adopting ML)
- Deliver innovative bespoke and industry leading technology solutions, including implementation of TM systems, AML model validation, and operating model transformation to improve the human and virtual workforce

We have vendor alliances, both with Fintech start-ups and with leading firms. Accenture consultants meet on a regular basis with new vendors, help vendors build their capabilities in the financial crime prevention space, and evaluate them to deliver greater value to clients. Within the financial crime space, Accenture has established an effective and efficient methodology to allow our clients to meet regulatory expectations and reduce volumes of TM and Name Screening alerts. This methodology is illustrated in Figure 6 below.

Figure 6. Summarized Steps for Rapid Benefits Realization from ML and RPA

<table>
<thead>
<tr>
<th>DEFINE OPPORTUNITIES</th>
<th>IDENTIFY DATA SOURCES AND SYSTEMS</th>
<th>SCOPE IMPLEMENTATION TRANCHEs</th>
<th>BUILD AND TEST ADVANCED ANALYTICS APPLICATIONS</th>
<th>ROLL OUT, MAINTAIN AND UPDATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Identify pain points</td>
<td>• Analyse available and required data</td>
<td>• Outline immediate, mid-term and long-term goals</td>
<td>• Enhance and fix data</td>
<td>• Periodically review and tune applications for ongoing suitability</td>
</tr>
<tr>
<td>• Identify processes and procedures that can be automated</td>
<td>• Perform data quality analysis (e.g. completeness ratios)</td>
<td>• Identify the &quot;art of the possible&quot; for automation and ML</td>
<td>• Algorithm and vendor selection</td>
<td>• User training and feedback to improve usability</td>
</tr>
<tr>
<td></td>
<td>• Build a consolidated data repository</td>
<td>• Develop delivery approach and road map</td>
<td>• Build, deploy and test proofs of concept</td>
<td></td>
</tr>
</tbody>
</table>
Within the financial crime space, Accenture has established an effective and efficient methodology to allow our clients to meet regulatory expectations and reduce volumes of TM and name screening alerts.
CONCLUSION

Many banks have started implementing business process automation in the form of RPA and see AI and particularly ML as the next step in the journey to greater efficiency and effectiveness. Some banks, however, believe they should walk before they run, meaning that robotics solutions should be in place before AI ML solutions are considered.

In fact, robotics and AI ML can exist independently of each other and each can support the other’s capabilities. Robotics can be used to train AI ML models and AI ML models can be used to add decision-making (in the form of NLP) or reading (via optical character recognition) capabilities to robotics models.

The appetite for automation is increasing rapidly, but challenges remain. Implementing ML may improve event-to-SAR conversion rates but there will always be a need for human involvement. Hybrid human/AI models are likely to appear in the near future and should represent the next generation of AML TM alert operations teams. The adoption of ML and, ultimately, AI in AML is only the beginning of financial services compliance and resilience automation.
ABOUT THE AUTHORS

**Samantha Regan**
Samantha is a Managing Director, and is the North America Lead for the Regulatory Remediation & Compliance Transformation group within Accenture’s Finance & Risk practice. Based in New York, she has 17 years of global experience working with C-suite executives and their businesses in compliance and regulatory initiatives.

**Heather Adams**
Heather is a Managing Director, Accenture Finance & Risk. Based in London, she leads Accenture’s UK & Ireland Resilience team, developing capabilities and supporting clients in their efforts to be resilient to a range of external and internal threats, including financial crime. Heather has extensive experience in delivering large-scale complex business change for banks and has worked with senior leaders to define and implement financial crime risk strategies to drive high performance.

**Philippe Guiral**
Philippe is a Senior Manager, Accenture Finance & Risk, based in New York. He leads Accenture’s North America Financial Crime Group, and has over 12 years of experience, defining capabilities and strategies to support clients in their financial crime prevention programs in both the UK and the US. Philippe specializes in delivering large-scale complex business and technology financial crime change programs to drive high performance.

**Saad Choudri**
Saad Choudri is a Technology Consulting Principal, Accenture Finance & Risk, based in London. Saad has over 12 years of international multisector experience as a change professional with a special focus on financial crime prevention and artificial intelligence.
The appetite for automation is increasing rapidly, but challenges remain. Implementing ML may improve event-to-SAR conversion rates but there will always be a need for human involvement.
REFERENCES


2. FinTech Innovation Lab, London: http://www.fintechinnovationlablondon.co.uk/

ACKNOWLEDGMENTS

The authors would like to thank the following Accenture employees for their contribution to this document:
Garikai Mparutsa
Zhana Gali

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 411,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Its home page is www.accenture.com

DISCLAIMER

This document is intended for general informational purposes only and does not take into account the reader’s specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.
EVOLVING AML JOURNEY

OPERATIONAL TRANSFORMATION OF ANTI-MONEY LAUNDERING THROUGH ROBOTIC PROCESS AUTOMATION
The regulatory burden on financial institutions (FIs) has increased dramatically in recent years. In the crucial area of Anti-Money-Laundering (AML) compliance, FIs have stepped up their spending on headcount to support Know Your Customer (KYC) activities and other key functions that require manual processing such as AML Customer Screening and Transaction Monitoring.

FIs are spending, on average, $60 million per year to meet their AML compliance costs, but some larger firms are spending up to $500 million annually to comply with KYC and Customer Due Diligence (CDD) rules.1 Back in 2015, we were estimating a 50 percent increase in costs related to AML over a three-year period.

Firms that fail to make the changes to meet regulatory demands run the risk of major reputational and financial losses (from 2010 to 2015, banks paid over $300 billion in fines related to non-compliance).2 The combination of high transaction volumes and increased regulation places a premium on an organization’s ability to streamline operations and maintain appropriate levels of control.

FIs are searching for new ways to reduce the costs of operational processing while remaining compliant in their AML programs. They have explored solutions across the Operational Transformation journey (Figure 1) including standardization, centralization, outsourcing and automation with varying degrees of success. However, experience has shown that leveraging a combination of centralization and automation alongside outsourcing solutions has resulted in significant cost reduction, as much as 15 to 35 percent across the enterprise.

Within the category of automation, the implementation of Robotic Process Automation (RPA) is showing potential for reducing costs and increasing the effectiveness of key AML and KYC activities. While RPA is not a silver bullet solution, if used with the right processes and avoiding common pitfalls, it can be quite beneficial.

Figure 1. The Operational Transformation Journey in AML

<table>
<thead>
<tr>
<th>STANDARDIZING</th>
<th>CENTRALIZING</th>
<th>OUTSOURCING</th>
<th>AUTOMATING</th>
</tr>
</thead>
<tbody>
<tr>
<td>• End-to-end Operational Process Design</td>
<td>• Offshoring</td>
<td>• Managed Services</td>
<td></td>
</tr>
<tr>
<td>• Technology Enhancements</td>
<td>• Center of Excellence</td>
<td>• Vendor Solutions (e.g. KYC Utilities)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Robotic Process Automation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Machine Learning</td>
<td></td>
</tr>
</tbody>
</table>

Source: Accenture, September 2017
THE CASE FOR RPA IMPLEMENTATION IN AML

Banks that leverage RPA can help lower costs, increase throughput and improve quality, while remaining compliant across the AML ecosystem. Our experience indicates that Robotics help deliver payback on investment in about three to six months when implemented at scale.

Additional key advantages and benefits can be found in Figure 2 below.

Figure 2. Key Advantages and Benefits of RPA Implementation

- Increased productivity with the potential to operate 24/7 – less FTEs needed to complete repetitive tasks
- New operational ability to dynamically manage resource capacity and address peak volumes
- One “bot” equates on average to 3 – 5 FTEs at about 1/3 the cost of an offshore resource
- Consistent quality delivered as human error is eliminated
- Approximately 6 – 8 weeks required for a cost-effective implementation
- Higher staff satisfaction by eliminating monotonous tasks and allowing individuals to focus on higher value work
- One “bot” equates on average to 3 – 5 FTEs at about 1/3 the cost of an offshore resource

Source: Accenture analysis, September 2016
SIX KEY CONSIDERATIONS FOR AN RPA IMPLEMENTATION

For an effective RPA implementation, FIs should be aware of six key considerations, which can help them avoid the pitfalls and mistakes that commonly occur during automation.

1. ANTICIPATED BENEFITS

The benefits derived from automating a specific process can vary greatly depending upon the FI and the process in question. Elements to consider include the potential FTE (full-time equivalent) savings (or avoiding the need to hire more FTEs); the time required for payback or break-even point on the investment; the expected increase in operational throughput and/or quality; and qualitative benefits such as improvements in the customer experience or faster realization of revenue.

2. VENDOR ALIGNMENT

The process being automated should align with offerings available from current or potential robotics vendors used by the firm. Potential differentiating factors that influence the vendor decision include cost, compatibility, ramp-up speed, capacity to scale up, and ability to provide ongoing maintenance. In addition, some vendors have areas of specialization which should be taken into account during the vendor selection process.
3. PROCESS COMPLEXITY

In addition to being high volume and repeatable, processes selected for automation should be stable and operating effectively. Attempting to automate a poorly-designed process often results in a failed or prolonged implementation. In some cases, it is beneficial to perform some re-engineering to address process opportunities before attempting to automate. All processes should be identified, assessed and prioritized using a consistent intake methodology across the firm. Additional process selection considerations include the number of stakeholders/owners within a process (less is better) and the sustainability of the process.

4. TECHNOLOGY MATURITY

The automation of a process utilizing strategic target state platforms is less burdensome and in our experience, requires less ongoing maintenance than a process dependent on multiple legacy systems and offline data sources (such as spreadsheets). Additionally, firms should hold off on automating any processes impacted by an in-flight technology transformation, as this delays a robot going to production or may render a newly developed robot obsolete.

5. OVERSIGHT

Robots also require ongoing maintenance as data sources (internal and external) and key systems change. This maintenance is essential as it allows bots to continue to perform consistently and accurately. It is also essential to have a robust incident management process, including root cause analysis for RPA defects. Subject matter specialist involvement from the lines of business (LOBs) is also crucial before, during and after bot implementation.

6. IMPACT UPON EMPLOYEES

There is a common perception that robots will eventually take away most human jobs, but this is misguided. Robots will never replace the need for human oversight, judgement and problem solving. It is essential for firms to communicate this to employees as the utilization of robotics impacts morale. Ways to keep employee engagement high include: participation in the identification, assessment and prioritization of processes for automation and training employees to support configuration of robots as well as the ongoing maintenance of those robots. Employees should not feel threatened by robots, but rather, empowered to support the firm in this step of the transformational journey.
THE APPLICABILITY OF RPA FOR AML

Most processes within the AML ecosystem involve a similar set of activities based upon the research, validation, evidence and upload of customer information.

RPA-based solutions are well-equipped to incorporate these activities into an overall AML operational transformation program. Some of the key use cases within AML include CDD, client screening, transaction monitoring and client offboarding. These are all well-suited to benefit from the implementation of RPA capabilities.

1. Customer Due Diligence. Use cases within CDD include client setup, onboarding, refresh and enhanced due diligence. During refresh, for example, RPA can be used to validate existing client information, pulling client data from various internal repositories to verify the client’s information or to hand off to an associate for review. With several internal and external sources available for client verification, RPA can be leveraged to search internal data repositories as well as approved third-party data sources for client information. RPA can also automatically send emails to frontline staff and clients, requesting necessary KYC documentation.

RPA can also be used to capture screenshots of the client information that was collected and verified, and based on the information received during the onboarding or refresh processes, it can manage further due diligence based on the customer's risk level.

2. Client Screening. RPA use cases in client screening include sanctions/OFAC, Politically Exposed Persons (PEP) and adverse media screening. For example, RPA can help compile and consolidate customer information from multiple databases and hubs and send to screening vendors or compare directly to watch lists. RPA can also perform first level reviews and determine if screening results are "hits" or "false positives" based on predetermined business rules. As is the case with CDD, RPA can manage screening based on the client’s risk level.

3. Transaction Monitoring. The most important use case in transaction monitoring is alert review. Screening systems can generate thousands of duplicate alerts that are then closed by investigators using previous case closure evidence. RPA can identify repeated alerts, check for changes in status, and take action to close without involving the investigator. RPA can also manage the data collection process for suspicious transaction alerts, handing off to associates to review or closing the alert on its own, based on predetermined business rules.
This eliminates mundane reviews and data gathering for associates, leading to fewer human errors and a clearer focus on the highest risk customers and transactions.

Many FIs struggle with a lengthy alert backlog. An analytics-based method can be used to detect and aggregate false positives, with RPA taking output from this analytics solution to update and close cases in bulk.

4. **Offboarding.** Institutions determining when to close accounts or when to place a customer on a Do Not Do Business (DNDB) list can use RPA to check the client’s account status and provide insights on account activity. RPA can take over the manual process of updating restriction and/or closure codes to help eliminate human error and automate routine tasks. Based on business rules, RPA can proactively monitor and prevent transactions with specific clients on the DNDB list.

This table shows specific RPA capabilities and how they can be applied to key AML functions.

**Table 1. Mapping AML Suitability**

<table>
<thead>
<tr>
<th>AML Function</th>
<th>Key Capability</th>
<th>CDD</th>
<th>Client Screening</th>
<th>Transaction Monitoring</th>
<th>Offboarding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Aggregation</td>
<td>Internal/External Research</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Validating Client Information</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Documentation of Evidence</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Update Case Status</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Check Account Status</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

Source: Accenture, September 2017
RPA is an important step in the operational transformation journey of AML, but newer technologies, such as Machine Learning and Artificial Intelligence, are expected to build upon and expand the horizons of automation.

Transaction monitoring, for instance, currently relies on the development of hundreds of business rules to detect patterns in the deposit, transfer and withdrawal of funds from an FI. Machine learning can be utilized to analyze large quantities of transaction data to detect anomalies and patterns, without having to work within the confines of business rules that are often outdated. Machine learning can also support the auto-triage and enrichment of alerts with information from internal sources. This information may be retrieved more efficiently than it can by investigators manually running online web searches.

Poor data quality or a lack of useable data can affect decisions made by machine learning models, as can a lack of information-sharing between regulators and banks. Another hurdle includes the lack of trust regulators have in decisions made by machine learning models. Unlike RPA, which can be implemented quickly and inexpensively, there may be difficulties in integrating machine learning solutions with existing systems and tools. For more information on machine learning applicability for AML, please see our thought leadership piece titled “Leveraging Machine Learning within Anti-Money Laundering Transaction Monitoring.”
CONCLUSION

As FIs continue to transform their operations to keep up with the ever-changing AML landscape, RPA should be a key part of that transformation. Through RPA, we are seeing organizations drive down their operational costs, while meeting or exceeding throughput targets, maintaining high quality, and remaining compliant. With proper leadership and governance, and through the selection of processes that are well-suited for automation, FIs are realizing a major operational uplift from RPA in a relatively short amount of time.
HOW ACCENTURE CAN HELP

Accenture has a leading Financial Crime and AML practice with an integrated global network of deeply skilled professionals. Accenture is an industry thought leader, possessing proven methodology and extensive experience in AML/KYC remediation and transformation engagements working with major banks and technology company in Canada, the US and Europe.

Accenture is also well positioned to provide integrated RPA solutions with over 1000 robotics specialists across the globe, key relationships with the top 5 RPA providers and an ecosystem of collaborative alliances.

ABOUT THE AUTHORS

Samantha Regan
Samantha is a Managing Director, and is the North America Lead for the Regulatory Remediation & Compliance Transformation group within Accenture’s Finance & Risk practice. Based in New York, she has 17 years of global experience working with C-suite executives and their businesses in compliance and regulatory initiatives.

Philippe Guiral
Philippe is a Senior Manager, Accenture Finance & Risk, based in New York. He leads Accenture’s North America Financial Crime Group, and has over 12 years of experience, defining capabilities and strategies to support clients in their financial crime prevention programs in both the UK and the US. Philippe specializes in delivering large-scale complex business and technology financial crime change programs to drive high performance.

David DeLeon
David is a Senior Manager, Accenture Finance & Risk. Based in Charlotte and focused on banking and risk, he is a member of the Financial Crime group and is the AML Managed Services Offering Lead for North America. David has led transformational programs across retail, wealth management, and wholesale banking and helped North America clients with their AML strategy, regulatory responses, design and deployment of KYC operations teams, target operating model enhancements, and large scale technology implementations.

John Branisteau
John is a Manager, Accenture Finance & Risk, based in Charlotte. John is an experienced financial services consulting professional having worked on key strategic and transformational engagements with several top global banks. His recent focus has been on AML process and operating model design as well as robotic process automation evaluation for AML/KYC. Prior experience includes compliance risk framework development and enterprise GRC platform implementation and adoption.
Machine learning can be utilized to analyze large quantities of transaction data to detect anomalies and patterns, without having to work within the confines of business rules that are often outdated.
REFERENCES


ACKNOWLEDGMENTS
The authors would like to thank the following Accenture employees for their contribution to this document:

Garikai Mparutsa
Corey Hartley

STAY CONNECTED
Accenture Finance and Risk
www.accenture.com/financeandrisk

Finance and Risk Blog
financeandriskblog.accenture.com/

Connect With Us
www.linkedin.com/showcase/16183502/

Follow Us @AccentureFSRisk
www.twitter.com/AccentureFSRisk

ABOUT ACCENTURE
Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 411,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Its home page is www.accenture.com

DISCLAIMER
This document is intended for general informational purposes only and does not take into account the reader’s specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.