Data Usage and Protection and Intellectual Property Issues for CFTC Registrants

November 14, 2019

Steven Lofchie and Vivian Maese,
Partners, Cadwalader, Wickersham & Taft

54301340v2

Overview

- Financial institutions are increasingly focused on the use, protection and commercialization of confidential data.

- This presentation addresses data usage, data protection and intellectual property issues affecting CFTC registrants including:

  • legal limitations on the use of various types of data, including customer; financial; trading bids, offers and executions; and employee information;

  • usage restrictions imposed by intellectual property rights or by contractual confidentiality agreements;

  • requirements regarding data preservation and destruction, data breaches, and outsourcing arrangements;

  • registration issues arising from the sale of structured data (indices and algorithms); and

  • issues relating to the use of data provided by third parties.

Policy Interests May Be Inconsistent

Protection of Property Rights	VS	Limits on Assets in Which Rights May Be Asserted
Ability to Keep Trade Secrets	VS	Limits on Ability to Impose Non-Competes
Obligation to Maintain Confidences	VS	Obligation to Disclose
Obligation to Maintain Information	VS	Obligation to Keep Information Safe
Obligation to Analyze Information	VS	Obligation Not to Make Improper Determinations
Free Movement of Capital	VS	Limits on Sales That Impair National Interest

CFTC, SRO and State Law Requirements

CFTC Data Protection Initiative: Questions that the CFTC Asks of Itself

- Scope:
  - Data Inventory: Who, what, where, when and why of data collection.
- Access:
  - How is data received? Frequency? Alternative methods of access
- Security: Safeguards and internal controls for storing data:
  - Storage procedures
  - Encryption
  - Permissioned access
- Incident Response:
  - Impact and risk assessments
  - Notifications
- Retention
- Disposal
- Review, monitor and update.

CFTC Registrants:
Use of Data for Regulatory Purposes

- Account Opening
  - AML
  - KYC and Credit Analysis
  - Bylaw 1101
- Trade Review:
  - Wash sales; prearranged trades
  - Spoofing and other manipulative conduct
- Position limit compliance:
  - Monitoring positions
  - Aggregation of positions
- Reporting Requirements:
  - Ownership and Control Reports
  - Large Trader Reports

CFTC Restrictions On Use of Data

- CFTC GLBA Privacy Requirements
  - Privacy Notices
  - Opt Out Notices
  - Permitted Uses of Information
  - Safeguard requirements
- CFTC FCRA Requirements
- Prohibition on Trading on Basis of Misappropriated MNPI

- CFTC Supervisory Requirements

CFTC Record Creation and Maintenance Obligations

- CFTC Registrants are subject to broad record creation and record maintenance obligations:
  - CFTC Rule 1.31 is the principal rule applicable to record maintenance
  - CFTC Rule 1.35 is principal rule applicable to creation of trading records
- Required records depend on type of entity and activity:
  - FCMs and IBs: *See, e.g.,* CFTC Rules 1.31 – 1.37.
  - CPOs and CTAs: *See* CFTC Rules 4.23 and 4.33.
  - SDs: *See* CFTC Rules 23.201 – 23.203.
  - There are numerous other CFTC and Exchange Rules establishing particular record creation and maintenance requirements
- Required time period for record retention varies with the type of entity and the type of document.
- CFTC Registrants must use storage media that ensures the "authenticity and reliability" of stored records.

CFTC Data Safeguard and Disposal Requirements

- Obligation to establish procedures for safeguarding retail customer information:
  - Must address “administrative, technical and physical safeguards”
  - Procedures must be reasonably designed to:
    - Ensure data’s “security and confidentiality”;
    - Protect against “anticipated threats or hazards”; and
    - Protect against “unauthorized access to or use of” data “that could result in substantial harm or inconvenience” to any customer.
- Obligation to implement both protective measures as to stored dated and reasonable disposal measures to protect against unauthorized access.
- CFTC Data Safeguard Best Practices.
- Serves as key enforcement “hook” by CFTC, including recent enforcement actions designed to address cybersecurity weaknesses.

Identity Theft Prevention Program: CFTC Rule 162.30

- Is firm within scope?
- Requirements for in-scope firms to establish an Identity Theft Prevention Program
  - Identify Red Flags
  - Detect Red Flags
  - Respond to Red Flags
    - Investigating
    - Contacting Affected Customers
    - Notifying Law Enforcement
  - Approval by the Board of Directors
  - Appropriate Training
  - Regular Updating of the Program
  - Filing of Suspicious Activity Reports

CFTC Registration – When Does Data Become Commodity Trading Advice

- When does the provision of data become commodity trading advice?
- Does data qualify for the exemption from CTA registration for standardized advice in CFTC Rule 4.14(a)(9)?
- When does the provision of data become derivatives research for purposes of the CFTC Research Rules?
- What is the dividing line between an index and advice?

Overview of NFA Requirements

- Recordkeeping Requirements: NFA Compliance Rule 2-10
- Business Continuity Program: NFA Compliance Rule 2-38
- NFA Supervisory Requirements: NFA Compliance Rule 2-9

- NFA Interpretive Notice 9070: Information Systems Security Program
- NFA Interpretive Notice 9061: Prohibition on Misuse of Confidential Information
- NFA Interpretive Notice 9074: CPO Internal Controls

NFA Information Systems Security Program ("ISSP") Requirements

- Adopt written ISSP:
  - reasonably designed to safeguard against security threats to I.T. systems.
- Approval of ISSP Program by designated information security officer:
    - senior level officer with primary responsibility for I.T. system security;
    - other senior official who is a listed principal with authority to supervise the firm's ISSP.
  - Note: Personal liability issues
- Group-level ISSP permissible subject to conditions.
- Governance structure and escalation procedures to identify and manage security risks
- Risk Assessment
- I.T. Safeguards

NFA Information Security Systems Program Requirements (cont'd)

- Incident response plan
- Notice Requirements:
  - Notify NFA of cybersecurity incidents affecting the firm's CFTC-regulated business that result in:
    - any loss of customer or counterparty funds;
    - any loss of firm capital;
    - customer notification under State or Federal law.
  - No monetary threshold for loss of customer funds/firm capital.
  - SAR Filing Requirements for FCMs and IBs.
- Employee training: on hiring and (at least) annually thereafter
- Monitor and review ISSP at least annually
- Maintain records re. adoption and implementation of ISSP

Prohibits CFTC Registrants and their personnel from:

- Obtaining confidential information or trade secrets from another CFTC Registrant without permission;
- Misusing confidential information or trade secrets.

Examples of Prohibited Conduct:

- Misuse of sensitive personal information (e.g., social security number);
- Violating the firm's privacy policy;
- Disclosing customer orders prior to execution (except as permitted by exchange rules); or
- Obtaining a CTA's historical trading positions without the CTA's permission.

NFA Business Continuity Requirements

- Business continuity plan requirements include:

  – Back-up facilities and systems;
  – Data back-up and recovery;
  – Minimize impact of business interruptions affecting third parties;
  – Parties to contact in event of business interruption
  – Periodic update, review and testing of plan;
  – Informing relevant personnel of responsibilities under plan.

  See NFA Compliance Rule 2-38; NFA Interpretive Notice 9052.

Derivatives Exchanges: Restrictions on Disclosure of Trading Information

- Derivatives exchanges impose significant restrictions on sharing confidential trading information. These include:
  - Restrictions on pre-execution communications.
  - Restrictions on disclosure of non-public order information.
  - Restrictions on disclosure of non-public information regarding block trades.

Outsourcing: Regulatory framework

- Outsource functions, not regulatory responsibility.
- CFTC Registrant retains ultimate responsibility for supervisory and compliance responsibilities.
- CFTC Registrants may not outsource activities that require CFTC registration.
- Enterprise-wide policies and procedures should be in place to ensure proper risk management of independent contractors and other third party vendors.
- Third-party vendor relationships should be properly structured and managed, in compliance with relevant policies and procedures, and firms should ensure that outsourcing arrangements are adequately supervised and documented.

Outsourcing: Due Diligence

- Proper diligence in determining whether a third-party is qualified to perform services includes:
  - Considering the vendor's financial viability, reputation, and fitness for the services in question;
  - Performing a risk assessment of impact on the firm and its customers if the vendor fails to perform the contemplated services;
  - Assessing whether appropriate internal controls related to the specific services provided are maintained by the vendor;
  - If the service provider in turn sub-contracts key services, reviewing the ability of any sub-vendor to perform services material to the performance of the outsourcing contract; and
  - Assessing effectiveness of the service provider's cybersecurity protections, privacy and confidentiality controls, and general data protection.
- Outsourcing arrangements should be drafted to maintain the ability to conform to changes in regulatory requirements on an ongoing basis.

CFTC Cyber Enforcement Actions

- *Phillip Capital*, CFTC Settlement Order (Sept. 12, 2019).
- Hackers breached FCM's email system, accessed customer information, and withdrew $1m in customer funds.
- Alleged Supervisory Failures under CFTC Rule 166.3
- Alleged Disclosure Failure: CFTC Rule 1.55(i)
- Sanctions:
  - $1m restitution (previously paid by firm on discovery of breach);
  - $500k civil monetary penalty.

CFTC Cyber Enforcement Actions

- *AMP Global Clearing LLC*, CFTC Settlement Order (Feb. 12, 2018).
- I.T. provider installed a network storage device into the FCM's network that allowed open access via the internet.
- A third party accessed the network and copied approximately 97,000 files that included customers' personally identifiable information.
- The third party contacted federal authorities about securing the copied information.
- Alleged Supervisory Failures under CFTC Rule 166.3
- Sanctions: $100,000 civil monetary penalty.

CFTC Cyber Enforcement Actions

- *Tillage Commodities*, CFTC Settlement Order (Sept. 28, 2017).
- Hackers spoofed email account of CPO's managing member, and sent pool administrator 7 fraudulent requests to transfer sums from commodity pool bank account to third-party accounts.
- The pool administrator processed 5 of the fraudulent requests over a 3-week period, resulting in a loss of $5.9m (64%) of pool funds.
- Following discovery of fraud, CPO immediately offered investors the option to redeem.
- Alleged Supervisory Failures under CFTC Rule 166.3
- Sanctions: $150,000 civil monetary penalty.

State Law Requirements (*e.g.*, NYDFS Cybersecurity Requirements for Financial Services Companies)

- Scope of Coverage
  - Is firm within scope?
  - Covered information not limited to personal information; any information whose disclosure "would cause a material adverse impact ot the covered entity's business"
- Scope of Cybersecurity Policy
  - Information Security
  - Appointment of Chief Information Security Officer & Data governance
  - Data Retention
  - Customer Privacy
  - Encryption
  - Device management
  - Business Continuity
  - Risk Assessment; Penetration Testing
  - Incident Response
  - Vendor Controls
  - Notices to NYDFS Superintendent (Stricter than general NY Statute on Data Breach)
  - Certifications

FTC Proposal on Cybersecurity and Information Safeguarding

- In March 2019, the FTC proposed more detailed requirements "based on the cybersecurity regulations issued by the New York [DFS] and the insurance data security model law issued by the National Association of Insurance Commissioners." In particular, the proposed amendments would include:
  - Chief Information Security Officer (CISO) Requirement
  - Annual CISO Report to Board of Directors Regarding the IT Program
  - Detailed Incident Response Plan
  - Testing of Security Systems
  - Encryption
  - Risk Assessment and Auditing
  - Training and Education
  - Periodic Review of Service Providers
- CFTC has not currently issued similar proposal.

California Consumer Privacy Act

- Right to Know What Personal Data is Collected (Section 1798.100)
- Right to Delete Data (Section 1798.105)
- Right to Know Sources and Purposes of Collection (Section 1798.110)
- Right to Know Categories of Third Parties With Whom Information Will Be Shared (Section 1798.110)
- Right to Know About Sale of Information (Section 1798.115)
- Right to Prohibit Sale of Information (Section 1798.120)
- Prohibitions on Discrimination Against Customers Exercising Statutory Rights (Section 1798.125)
- Right to Access Information (Section 1798.135)
- Requirement that Demand Data be Kept Safe (Section 1798.150)
- Law provides for private rights of actions (Section 1798.150)
- Does not apply to data that has been "deidentified" (*i.e.*, personal information that cannot identify, relate to, describe or be connected to a particular consumer)

Data Breach Notice Obligations

- All 50 States and District of Columbia Have Data Notification Laws
- Notice to Affected Customers Generally Must be Provided Promptly
  - States have explicit deadlines for notifying affected individuals
  - States may require notice to State Government; *e.g.*, Attorney General
  - States may require a specific form of notice
    - California requires that the notice be titled Notice of Data Breach
- Data covered by State Laws Varies
  - Name, Financial Information, Health Information, Credentials
- Potential for Private Rights of Action
- Related Notification Requirements, e.g., NFA Notice under the ISSP Interp.

Data Breach Notice Obligations (cont'd)

- Fallout from recent high-profile breaches (Equifax, Yahoo, etc.) has led Congress to hold hearings on data breach and related notification obligations
- Various proposals over the years on a uniform data breach notification law, but no immediate prospects of passage
- What will be the key terms of any proposed legislation:
  - Which entities will be covered and how will "personally identifiable information" be defined (SSN, account numbers, unique biometric data, etc.)?
  - What are the time limits for notification to regulators or other authorities (72 hours of breach notification, etc.), notices to customers (30 days, etc.)? Which regulators/authorities?
  - How will it compare with other standards, such as the EU's GDPR framework?
  - What are the content requirements for a customer breach notice?
  - What are acceptable consumer notification methods (traditional written notices, e-mail notices, use of major media outlets, etc.)?
  - Will there be any safe harbors?
  - What will be the effect on related state laws; e.g. preemption?

State Data Disposal Regulations

- The majority of states govern the manner in which personal information is disposed.
- Generally applies to “Personal Information” or “Consumer Information” or “Personal Identifying Information”
- Specifies a number of appropriate means of disposals:
  - Shredding
  - Destroying information in the records
  - Altering Information to make it unreasonable

European Union General Data Protection Regulation

- Right to Access Information
- Right to Have Information Corrected
- Right to Have Information Deleted (“Right to be Forgotten”)
- Right to Restrict Access
- Right of Portability
- Right to Object
- Rights in Relation to Automated Decision Making

OWNERSHIP RIGHTS

Intellectual Property (Asserting Rights in Property):

- Copyright
- Trade Secret
- Patent
- Misappropriation
- Contract
  - Customers
  - Data Providers
  - Data Users
  - Other Vendors
  - Employees

Considerations regarding Use of Data

- To whom does the information belong:
  - Futures customers and swap counterparties
  - Executing brokers, clearing firms and prime brokers.
  - Government officials and regulators
  - Vendors and service providers
  - Data created by algorithms or predictive analysis
- Are you free to use it:
  - How is use of data regulated?
  - Confidentiality issues
  - Trading Restrictions (e.g., front-running or pre-hedging)

Copyright

General Copyright Law

- Copyright protection subsists in original works of authorship fixed in any tangible medium of expression (17 USC 101(a)).
- The owner of a copyright has exclusive rights to reproduce, distribute, publicly perform or display, and create derivative works based upon, the copyrighted work (17 USC 106).

Protections Generally Not Apply to Data Alone

Copyright (cont'd)

Limited Protection for Compilations of Data

- Protection will apply to a compilation if the data are "selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship" (17 USC 101, 103).

Trade Secret

General Trade Secrets Law

- Most states have adopted or closely follow the Uniform Trade Secrets Act, which defines a trade secret as any "information, including a formula, pattern, compilation, program, device, method, technique or process that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."
- The federal *Economic Espionage Act* (18 USC 1831 *et seq*.), which provides criminal penalties for certain trade secret thefts, uses a similar definition.

Can Protect Data and Compilations Data

Difficult to Apply to Widely-Distributed Data

Patent

General Patent Law

- The US Patent Act applies to the invention or discovery of “any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof” (35 USC 101).

Not Applicable to Data as Such

- Data and information do not qualify for patent protection.
- Inventions that relate to information processing or storage may be patentable if they are sufficiently nonobvious and meet the standards for novelty, but that protection would not otherwise apply to the data that is so processed or stored.

Misappropriation

General Misappropriation Law

- Misappropriation is a tort concept that applies unfair competition and equitable principles to protect against commercial "free riding" off the efforts of others.
- Its origin traces to *International News Services v. Associated Press*, 248 US 215 (1918), where the Supreme Court determined that one news agency should not be permitted use a another agency's newsfeed to generate competitive news services. "[D]efendant is endeavoring to reap where it has not sown."

Can Provide Quasi-Intellectual Property Protection for Data and Data Compilation

- Its reliance on the unfairness of profiting from the efforts of others is akin to the "sweat of the brow" protection that is rejected by US Copyright Law.
  - COMPARE: *EU Data Database Directive 96/9EC* – Provides *sui generis* protection for databases that are based on a substantial investment of resources, time, effort and energy in obtaining, verifying or presenting their contents.

Can Provide Quasi-Intellectual Property Protection for Data and Data Compilation

Problematic Preemption Issues May Limit to "Hot News" Only

Prohibition on Trading on Basis of Misappropriated MNPI: CFTC Rule 180.1.

Contract

General Contract Law

- So long as a contract does not violate law or public policy and is otherwise properly formed, courts will readily enforce to give effect to the intention of the parties as expressed in their agreement.

Contracts are typically required by data and information service providers as the most reliable form of legal protection

Key Issues in Data Contracts (for Users)

General Data Use Rights

- Many vendor data services are for “internal use only.”
  - Consider inclusion of affiliates
  - Watch for restrictions limiting use by and/or distribution to specific locations, personnel, departments, or lines of business
- Be clear about any external redistribution rights you may expect or require.
  - Data contracts often treat the vendor data as confidential information that is subject to non-disclosure requirements that effectively prohibit disclosure to third parties
  - Vendors often include or will give an express right to redistribute “limited amounts or data in the ordinary course of business.” More expansive redistribution rights ordinarily require special agreements
  - Watch for vendor attribution requirements, mandatory disclaimers, or provision requiring agreements/clickthrough terms for recipients of redistributed vendor data

Rights Relating to Resultant Data

- Resultant (or “Derived”) data refers to information that is created using the raw vendor data as an input.

Data Purge Requirements

Top 5 Questions for Assessing Data Usage

1. **What are the Sources of Data (*e.g.*, how was the data created or delivered)?**

2. **How is Data Collected?**

3. **What Type of Data Is It?**.

4. **Are there Policies and Procedures in Place to Separate or Restrict or Prohibit Access and Uses?**

5. **How is the Data Flow and Data Use being Reviewed and Supervised?**

Additional Methods of Protecting Data
Employee Covenants

Employees in the U.S. are frequently subject to restrictive covenants as a condition of employment (usually located in employment agreements, standalone restrictive covenant agreements, or in an employee handbook)

Although the classic justification for these types of restrictive covenants is to preserve trade secrets and prevent unfair competition, the use of such covenants can also have the ancillary effect of helping companies comply with data privacy laws by providing a contractual avenue for enforcement against individual employees

Some common types of restrictive covenants:

- Confidentiality
- Intellectual Property
- Return of Property
- Non-competition
- Non-solicitation of customers and employees

DATA DISTRIBUTION AND DUE DILIGENCE

Data Distribution Due Diligence

Check Third-Party Data Source Rights

- *Bloomberg v. UBS*, SDNY 18-CV-06334 (filed July 12, 2018): Bloomberg sues UBS for alleged violation of data service contract by redistributing data through its client-facing "UBS Delta" portfolio analysis and risk management platform.
- Key facts alleged by Bloomberg are:
  - UBS signed 1998 data license agreements that prohibit use of the data "in a manner that would result in licensee effectively becoming a source of or substitute for Bloomberg's proprietary data, or in a manner that would result in the licensee competing with Bloomberg."
  - The licenses were amended in 2005 to grant to UBS (for $300K/yr.) the limited right to use select Bloomberg data "within certain UBS software products that were made available to third party clients of UBS." Those amendments, however, reaffirmed the substitute/compete restrictions of the 1998 agreements.
  - In 2017, Bloomberg learns that StatPro announced an agreement with UBS to acquire the UBS Delta system subject to a 3 to 5 year transition period.
  - Bloomberg later determines that UBS violated its agreements with Bloomberg by (i) allowing UBS Delta clients to access a "vast trove" of Bloomberg data, and (ii) transferring to StatPro UBS employees having access to Bloomberg terminals and data.

Data Distribution Due Diligence (cont'd)

Key Take-Aways for Data Distribution Diligence

- *Good diligence begins with the data source contracts*.
- *The specific terms of the contract must be carefully parsed*.
- *It's not just the raw vendor data that needs to be considered*.
- *Consider the contract terms beyond just data use and distribution rights*.

Data Distribution Due Diligence (cont'd)

Apply Appropriate and Enforceable User Agreements

- A well-crafted user agreement is considered the most reliable form of legal protection for your proprietary data.
- Click-through and shrinkwrap agreements are generally enforceable.
- It is important to consider whether the individual signing or otherwise executing the agreement on behalf of an institutional user has the actual or apparent authority to do so.
  - *Determining authority can be fact-intensive*
  - Note: Arguably, an agreement that may initially be voidable for lack of authority can become enforceable through a later course of conduct demonstrating the principal's awareness of, and continued acceptance of benefit under, the subject agreement.

Steven Lofchie

Steven Lofchie
Partner
New York
Tel +1 212 504 6700
steven.lofchie@cwt.com

Steven Lofchie, a partner in the Financial Services Group at Cadwalader, Wickersham & Taft LLP, advises financial institutions on regulatory issues and financial instruments. His regulatory practice encompasses the securities laws, the CEA and related bankruptcy issues. His transactional practices focuses on securities credit and derivative transactions.

Profile

Chambers USA has ranked Mr. Lofchie in its first band, for seven years running, for both financial services regulation and derivatives, the only lawyer in the country to be top-ranked in both these categories. The 2017 edition of *The Best Lawyers in America* recognized Mr. Lofchie as Lawyer of the Year for Administrative/Regulatory Law in New York, and *U.S. News and World Report* ranked him as the best regulatory lawyer in New York for 2014. In 2012, a derivatives transaction developed by Mr. Lofchie was named as the best international structured product of the year by *International Financial Law Review*.

Mr. Lofchie is the founder and manager of the Cadwalader Cabinet, an acclaimed legal website that has been endorsed by former Chairpersons of both the SEC and CFTC. See www.findknowdo.com. Subscribers to the website include government regulators and major buy- and sell-side firms.

Mr. Lofchie received his B.A. from Sarah Lawrence College and his M.B.A. from Columbia Business School, where he was a General Motors Fellow. He received his J.D. from Yale Law School, where he was a member of the *Yale Law Journal*. He is also a contributor to the Center for Financial Stability, a leading nonpartisan think tank.

Vivian Maese

Vivian Maese
Partner
New York
Tel +1 212 504-5555
Vivian.Maese@cwt.com

Vivian Maese focuses on strategic and corporate transactions and projects (M&A, JV, spinouts, consortia, commercialization of IP) in the financial services industry with an emphasis on technology, IP, data, trading, regulation and compliance. Vivian advises clients, ranging from bulge-bracket financial institutions to emerging companies, on matters at the intersection of financial services regulation and technology; as well as on technology innovations in financial services, such as blockchain, crypto assets and artificial intelligence. She helps her clients build, maintain and extract value from their businesses.

Prior to joining Cadwalader, Vivian was a partner at Latham & Watkins and co-chaired the firm's Financial Institutions and Fintech industry groups. She also served as general counsel and corporate secretary at BIDS Trading, a financial services industry consortium for equities trading, and provided oversight on all legal issues related to U.S. cash trading and market data for the New York Stock Exchange. Vivian spent more than 20 years at Salomon Brothers and Citigroup, where she worked her way up through the ranks to become a divisional general counsel and managing director. She was the lead lawyer on many corporate transactions and technology initiatives, including the Fulcrum Project, which transformed electronic trading on Wall Street.

Vivian is top-rated in all the major directories and was named Band 1, the highest ranking possible, in Chambers & Partners Professional Advisors Fintech ranking for 2019. She has been recognized repeatedly for her accomplishments. Most recently, Vivian was named a FinTech, Blockchain and Cryptocurrency Trail Blazer by the *National Law Journal*. In addition, Vivian was nominated by her clients and received the Markets Media Women in Finance Award. In 2018, she was named to the Women in Fintech Powerlist and the *Financial Times* named Vivian as a Top 10 Innovative Individual in its *North American Innovative Lawyers* report in 2016.

Vivian Maese (cont'd)

Throughout her career Vivian has been very active in the community. In 2018, she was named Humanitarian of the Year by the Hope for a Healthier Humanity (78) Foundation, which provides resources to cultivate better health care infrastructures, offer education services and donate medical supplies to people in underdeveloped nations.

Vivian received her J.D. from Brooklyn Law School and her B.A. from Hunter College of the City University of New York. She is admitted to practice in the State of New York and is licensed to practice before the Supreme Court of the United States.