LOU PENN & Associates, Inc.
Market Conduct Auditor®

Company Violations for: All Companies

#	Cite Type	Ref #	State	Area Examined	Violation Category	Violation Date	Fine	Date Added	File Review Period Start	File Review Period End	Cite Title	Line of Business	Category	Compliance	Detail	Issue	Exam Type
1	Regulation	23 NYCRR 500.17	NY	Company operations and management	Companies violated the following sections of Cybersecurity Regulation: (1) the Companies' O365 email environments did not have multi-factor authentication ("MFA") fully implemented for all users until August 29, 2019, and no reasonably equivalent or more secure access controls than MFA were approved in writing by the Companies' Chief Information Security Officer(s) ("CISO"), in violation of 23 NYCRR § 500.12(b); (2) a misconfiguration error in MFA settings exposed a broad set of First Unum IP addresses to unauthorized third-party access in further violation of 23 NYCRR § 500.12(b); and (3) the company falsely certified compliance with Cybersecurity Regulation for the calendar year 2018, in violation of 23 NYCRR § 500.17(b).	5/14/2021	$ 1,800,000.00	5/14/2021	9/18/2018	5/14/2021	Notices to superintendent	All lines of business	Reporting Requirements	Annual/quarterly/monthly/statement/reports	Certificate of compliance/event reporting	Falsely certified compliance with the Cybersecurity Regulation	The Department has been investigating certain Cybersecurity Events, as defined by 23 NYCRR § 500.01(d), experienced within First Unum.
2	Regulation	23 NYCRR 500.12	NY	Company operations and management	Companies violated the following sections of Cybersecurity Regulation: (1) the Companies' O365 email environments did not have multi-factor authentication ("MFA") fully implemented for all users until August 29, 2019, and no reasonably equivalent or more secure access controls than MFA were approved in writing by the Companies' Chief Information Security Officer(s) ("CISO"), in violation of 23 NYCRR § 500.12(b); (2) a misconfiguration error in MFA settings exposed a broad set of First Unum IP addresses to unauthorized third-party access in further violation of 23 NYCRR § 500.12(b); and (3) the company falsely certified compliance with Cybersecurity Regulation for the calendar year 2018, in violation of 23 NYCRR § 500.17(b).	5/14/2021	$ 1,800,000.00	5/14/2021	9/18/2018	5/14/2021	Multi-factor authentication	All lines of business	Company Operations and Management	Cybersecurity requirements	Multi-factor authentication	Misconfiguration in MFA settings exposed IP addresses to 3rd parties	The Department has been investigating certain Cybersecurity Events, as defined by 23 NYCRR § 500.01(d), experienced within First Unum.
3	Regulation	23 NYCRR 500.12	NY	Company operations and management	Companies violated the following sections of Cybersecurity Regulation: (1) the Companies' O365 email environments did not have multi-factor authentication ("MFA") fully implemented for all users until August 29, 2019, and no reasonably equivalent or more secure access controls than MFA were approved in writing by the Companies' Chief Information Security Officer(s) ("CISO"), in violation of 23 NYCRR § 500.12(b); (2) a misconfiguration error in MFA settings exposed a broad set of First Unum IP addresses to unauthorized third-party access in further violation of 23 NYCRR § 500.12(b); and (3) the company falsely certified compliance with Cybersecurity Regulation for the calendar year 2018, in violation of 23 NYCRR § 500.17(b).	5/14/2021	$ 1,800,000.00	5/14/2021	9/18/2018	5/14/2021	Multi-factor authentication	All lines of business	Company Operations and Management	Cybersecurity requirements	Multi-factor authentication	Failed to have O365 email environments fully implemented for (MFA)	The Department has been investigating certain Cybersecurity Events, as defined by 23 NYCRR § 500.01(d), experienced within First Unum.