VENDOR'S CYBERSECURITY STANDARDIZATION TABLE

My LifeCard Plan®

GOVERNANCE AND RISK ASSESSMENT

SECURITY CONTROLS IN PLACE	DOES THIS CONTROL EXIST?	IF NO SUCH CONTROL (OR IF A CONTROL IS N/A), PLEASE EXPLAIN
1. Periodic cybersecurity risk assessments are conducted. Controls and risk management processes are tailored to the risks and vulnerabilities noted in your cybersecurity risk assessments.	X **Yes** ☐ No ☐ N/A	
2. An inventory of assets (people, hardware, applications / software, and data) authorized to access the firm's network is maintained. Assets are prioritized for the purposes of cybersecurity protection.	X **Yes** ☐ No ☐ N/A	
3. A written information security policy exists, has been reviewed within the past 12 months, and has been approved by management.	X **Yes** ☐ No ☐ N/A	
4. Written procedures exist for the protection of customer information.	X **Yes** ☐ No ☐ N/A	
5. A Chief Information Security Officer ("CISO"), or individual with similar responsibilities, exists and is focused on security.	X **Yes** ☐ No ☐ N/A	
6. A Cybersecurity Governance Committee (or group of similar function) exists and meets routinely to discuss items such as to cybersecurity risks, incidents, processes and related trends. Senior Management is provided a documented cybersecurity update at least quarterly.	X **Yes** ☐ No ☐ N/A	
7. A vendor management program exists that includes review of security practices of vendors with access to your network, premises, or data.	X **Yes** ☐ No ☐ N/A	
8. You maintain insurance that specifically covers losses and expenses attributed to cybersecurity incidents.	☐ Yes X **No** ☐ N/A	
9. A governance process exists to establish, implement, and actively manage (track, report on, correct) the system and security configuration of laptops, servers, and workstations using a consistent configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	X **Yes** ☐ No ☐ N/A	
10. Penetration testing is conducted by a 3rd party routinely / periodically (with the frequency determined by past results and risk assessments).	X **Yes** ☐ No ☐ N/A	

ACCESS RIGHTS AND CONTROLS

SECURITY CONTROLS IN PLACE	DOES THIS CONTROL EXIST?	IF NO SUCH CONTROL, PLEASE EXPLAIN
1. Security is simplified and automated for end users (e.g. they are not responsible for personally updating software and applying patches).	X **Yes** ☐ No ☐ N/A	
2. A user IDs and passwords policy and related procedures exists. Passwords are not shared and are regularly forced to be reset.	X **Yes** ☐ No ☐ N/A	
3. Login credentials of former employees are deleted immediately.	X **Yes** ☐ No ☐ N/A	
4. Authentication of users (via all methods include SSO) is secure.	X **Yes** ☐ No ☐ N/A	
5. A process exists for managing administrative-level accounts. Admin accounts are prevented from use on unauthorized systems.	X **Yes** ☐ No ☐ N/A	
6. Dual-factor authentication is required to access administrative-level functions on the server.	X **Yes** ☐ No ☐ N/A	
7. A practice exists to discourage or prevent logging on to unsecured computers with privileged accounts. Administrative-level accounts are prevented from browsing the Internet.	☐ Yes ☐ No X **N/A**	
8. You maintain controls to prevent unauthorized escalation of user privileges and lateral movement among network resources.	X **Yes** ☐ No ☐ N/A	
9. Application whitelisting is employed on sensitive systems such as domain controllers and administrative hosts.	X **Yes** ☐ No ☐ N/A	

BUSINESS CONTINUITY AND DISASTER RECOVERY

SECURITY CONTROLS IN PLACE	DOES THIS CONTROL EXIST?	IF NO SUCH CONTROL, PLEASE EXPLAIN
1. There are documented and management approved business continuity and disaster recovery plans that address the effects of cybersecurity incidents and/or recovery from such incidents if one happens.	X **Yes** ☐ No ☐ N/A	
2. The business continuity and disaster recovery plans are tested routinely / periodically.	X **Yes** ☐ No ☐ N/A	

PHYSICAL ENVIRONMENT

SECURITY CONTROLS IN PLACE	DOES THIS CONTROL EXIST?	IF NO SUCH CONTROL, PLEASE EXPLAIN
1. There are industry standard and reasonable physical safeguards including: a. Data rooms and/or access to servers containing confidential information or client PII are locked and access is monitored; b. Laptops and desktops have encrypted hard drives; c. Access to data processing facilities are restricted by badge or key; and d. Doors and windows are secure (and monitored by alarms if applicable).	X **Yes** ☐ No ☐ N/A	
2. An environment for testing and development of software and applications is kept separate from your production environment.	X **Yes** ☐ No ☐ N/A	
3. Visitors are required to sign in, have a visitor badge, and be escorted.	☐ Yes ☐ No X **N/A**	MLCP software operates on a dedicated server housed at GoDaddy in Scottsdale, Arizona who maintain in-house security.

DATA LOSS AND PREVENTION

SECURITY CONTROLS IN PLACE	DOES THIS CONTROL EXIST?	IF NO SUCH CONTROL, PLEASE EXPLAIN
1. Confidential information and client data is encrypted when stored on your network or any potentially internet-accessible devices.	X **Yes** ☐ No ☐ N/A	
2. Confidential information and client PII is transmitted securely.	X **Yes** ☐ No ☐ N/A	
3. Application, OS, and security patches are installed immediately.	X **Yes** ☐ No ☐ N/A	
4. Antivirus and antimalware software is deployed across all systems / devices and attempts to remove or disable such software is monitored. If applicable, an anti-financial malware tool is utilized.	☐ Yes ☐ No X **N/A**	
5. The firms employs firewalls to protect data and assets.	X **Yes** ☐ No ☐ N/A	
6. Intrusion detection software is implemented and utilized.	X **Yes** ☐ No ☐ N/A	
7. Data exfiltration software is utilized. A practice exists of monitoring the volume of data / content transferred out of the organization.	☐ Yes ☐ No X **N/A**	
8. Accounts for users who have access to PII are protected.	X **Yes** ☐ No ☐ N/A	
9. The use of removable storage media is restricted and monitored.	X **Yes** ☐ No ☐ N/A	
10. Data / document retention practices are FINRA / SEC compliant (e.g. cybersecurity, books and records, etc.).	☐ Yes ☐ No X **N/A**	

DATA PRIVACY AND INTEGRITY

SECURITY CONTROLS IN PLACE	DOES THIS CONTROL EXIST?	IF NO SUCH CONTROL, PLEASE EXPLAIN
1. Controls exist to verify the accuracy and integrity of data managed by your organization/system(s).	X **Yes** ☐ No ☐ N/A	
2. Controls exist to ensure that data managed is received/sent by/to the appropriate organizations (i.e. that one party does not send/receive data that should not be received/sent from/to another party).	☐ Yes ☐ No X **N/A**	
3. Data input to a multi-organization/user system is subjected to checks that ensure data accuracy and that the privacy of such information is protected. Data which fail such checks, must either be (a) rejected with a notification of the rejection sent to the submitter (b) corrected and resubmitted or (c) suspended pending further investigation.	☐ Yes ☐ No X **N/A**	
4. Policies and procedures exist to ensure compliance with all data management related rules and regulations of FINRA, the SEC, and any other applicable regulatory body.	☐ Yes ☐ No X **N/A**	
5. A defined incident response process exists (and can be shared with us) for resolving data privacy and/or integrity issues. The process lists specific actions your organization takes in communicating with impacted clients, advisors, and applicable regulatory/law enforcement agencies in the addressing data privacy and integrity incidents.	☐ Yes ☐ No X **N/A**	

CYBERSECURITY INSURANCE

INFORMATION		
1. Name of Carrier	N/A	
2. Carrier Contact Information (Name / Phone / E-mail)	N/A	
3. Broker Contact Information (Name / Phone / E-mail)	N/A	
4. Policy #	N/A	
5. Policy Period	N/A	
6. Coverage Limits (Per Claim and Aggregate)	N/A	
7. First Party Coverage	☐ Yes	☐ No
8. Third Party Coverage	☐ Yes	☐ No
9. Remediation Coverage	☐ Yes	☐ No

HUMAN RESOURCES / TRAINING / COMMUNICATIONS

SECURITY CONTROLS IN PLACE	DOES THIS CONTROL EXIST?	IF NO SUCH CONTROL, PLEASE EXPLAIN
1. Cybersecurity training is provided to staff and vendors on a regular basis and is tailored by job function.	X **Yes** ☐ No ☐ N/A	
2. There is an "acceptable use policy" in place that stipulates constraints and practices that a user must agree to and follow in order to gain / maintain access to your network.	X **Yes** ☐ No ☐ N/A	
3. All access persons including staff and 3rd party contractors acting upon your behalf are aware of and able to execute procedures for responding to cybersecurity incidents.	X **Yes** ☐ No ☐ N/A	
4. Your firm has established, and regularly updates, an employee education program regarding cybersecurity. This program keeps all firm personnel abreast of the latest trends in cybersecurity and firm cybersecurity policies and procedures.	X **Yes** ☐ No ☐ N/A	
5. If applicable, a retail client cybersecurity communication program exists that communicates information and actions potentially useful for clients to employ in order to further protect them from cybersecurity vulnerabilities.	☐ Yes ☐ No X **N/A**	
6. If applicable, a financial advisor cybersecurity communication program exists that communicates information and actions potentially useful for advisors to employ in order to further protect them from cybersecurity vulnerabilities.	☐ Yes ☐ No X **N/A**	
7. Access persons, including new hires and anyone such as 3rd party contractors acting upon your behalf, undergo background screening prior to start date and are required to sign confidentiality and non-disclosure agreements.	X **Yes** ☐ No ☐ N/A	
8. There are defined processes for all access persons including new hires, transfers, and terminations that take into account cybersecurity implications. Account deactivation at the time of termination is done immediately.	X **Yes** ☐ No ☐ N/A	

INCIDENT RESPONSE

SECURITY CONTROLS IN PLACE	DOES THIS CONTROL EXIST?	IF NO SUCH CONTROL, PLEASE EXPLAIN
1. There is a management approved incident response program that manages a cybersecurity event or incident in a way that limits damage, increases the confidence of external stakeholders, and reduces recovery time and costs.	X **Yes** ☐ No ☐ N/A	
2. Incident management reports are created routinely (e.g. each 90 days) when applicable and provided to senior management immediately in the case of a known breach.	☐ Yes ☐ No X **N/A**	
3. Roles and responsibilities for escalating and responding to cybersecurity incidents are defined. Your incident response plan lists specific actions your organization takes in communicating with impacted clients, advisors, and applicable regulatory/law enforcement agencies in the addressing data privacy and integrity incidents.	☐ Yes ☐ No X **N/A**	
4. The firm maintains provisioning of credit monitoring for individuals whose personal information has been compromised; and reimbursement to customers for financial losses incurred.	☐ Yes ☐ No X **N/A**	
5. The firm's approach involves incorporation of current threat intelligence to identify the most common incident types and attacks.	X **Yes** ☐ No ☐ N/A	
6. The firm maintains eradication and recovery plans for systems and data.	X **Yes** ☐ No ☐ N/A	
7. The firm has incident investigation and damage assessment processes.	X **Yes** ☐ No ☐ N/A	
8. The firm is involved in industrywide, and firm-specific simulation exercises as appropriate to the role and scale of a firm's business.	X **Yes** ☐ No ☐ N/A	