Written statement of proposed testimony by Carlos Vazquez for the Consumer Protection and Financial Institution subcommittee hearing on Cyber Threats, Consumer Data, and the Financial System

Evolving cybersecurity threats:

Cybersecurity is and always will be in a state of change. Yesterday the threat was malware, viruses and malicious executables inserted into a company's network. Today, ransomware, social engineering and supply chain attacks are the threats of the day. Tomorrow will see more of the same, plus deep fake technology, quantum processing (which may allow for easy compromise of all current cypher technology), and yet-unknown vulnerabilities in current hardware and software deployed by security departments in all companies.

Security departments are tasked with ensuring their data is and remains Confidential, with Integrity and Available (CIA) for those that require access to the data. The cost to ensure the CIA of data is tremendous and will continue to grow as technology evolves to counter the threat of APT groups and the day-to-day hackers trying to gain access to our networks and data for financial gain.

All financial institutions, especially credit unions with limited technical skills and funding, will need to ensure their strategies, for the current year to 3 to 5 years out, will be adaptable to meet the constant change in the threat landscape that affects cybersecurity.

Consumer data protection challenges:

People, processes, and technology are the challenges credit unions face to ensure our members' data is protected from malicious actors. Statistics show that in the financial services industry, a massive shortage exists in skilled security professionals which are required to manage the sophisticated tools in use today. Technology will constantly be changing and improving to counter the threat landscape brought to us by the malicious actors bent on breaking into our networks, via whatever means available, to steal our data for their own financial gain. The technology will not get cheaper; thus, it will be a challenge for the smaller institutions to both acquire and maintain it.

Training of employees is a challenge as social engineering has become the cheapest method of late for the malicious actors to trick users into providing credentials required to access the networks. Constant training is not only an escalating cost but a challenge to implement because employees either become weary or immune to the visual reminders of cyber hygiene.

Regulatory requirements can also present a challenge to financial institutions, especially smaller credit unions. Many may not have the ability or finances to maintain dedicated departments to ensure regulations are understood and met. For those financial institutions who need to meet regulations such as GDPR, the cost will be enormous in how to manage individual requests for management of their personal data.

Vendor management is another challenge facing financial institutions. With the supply chain breaches of 2021, it has highlighted the need to redo contracts with vendors to ensure transparency of any breach affecting the vendor. Many financial institutions will assume they are transferring their risk to

their vendors when they provide their data to those vendors. Although the risk may be transferred to the vendor ultimately the risk stays with the financial institution as our members expect us to secure their data. Vendors must have the same regulatory requirements to ensure data remains secure as the financial institutions themselves.

With the constant news of a new breach or ransomware affecting third-party vendors it becomes imperative that vendors do not become relaxed in securing our members' data. Vendors could easily have a runbook that assumes a breach can be fixed by social media messages and the hope their breach is only today's news cycle and quickly forgotten. Our members financial well-being is not trivial to us and should not be trivial to the vendors that have access to the data entrusted to us by our members.

Effort by government agencies to Strengthen cybersecurity defenses:

Data sharing (breaches, new vulnerabilities / patching, Advance Persistent Threat (APT) information) is paramount in ensuring all financial institution security departments are up to date on all threats affecting their security landscape. CISA, Homeland Security and Financial Services Information Sharing and Analysis Center (FS-ISAC) all are doing a great job in disseminating said information in a timely manner. It does fall on the financial institutions to ensure they are part of the data sharing network.

Webinars, conferences, and summits all provide the same information sharing that is very important in staying current with the threat landscape. In several recent summits there was participation by CISA and Homeland Security as guest speakers or presenters. Having these agencies present at these gatherings is very helpful and important as the discussions presented provide either information needed or some form of reassurance that the government is standing with financial institutions in their battle against the malicious actors.

Strengths and weaknesses of the current legal framework governing data security and privacy in the financial sector

The National Credit Union Administration (NCUA) is seeking legislative authority to have oversight over Credit Union Service Organizations (CUSOs) and third-party vendors that offer services to credit unions. The NCUA' Chairman sits on the Financial Stability Oversight Council (FSOC). The NCUA is the only federal agency that currently does not have this statutory authority as it relates to vendors that serve banking organizations. We believe credit unions deserve a regulator with parity in this regard.

Canvas Credit Union (located in Colorado) is supportive of parity for NCUA with the other federal regulators if the NCUA shares its information with state Regulators. Further, as vendors move offshore or go public it becomes increasingly challenging to hold some critical vendors accountable when we expect information from them.