Prepared Testimony of Katie Hawkins
Public Hearing on LD 1977, "An Act to Create the Data Privacy and Protection Act"
Maine Judiciary Committee
October 17, 2023

Good morning, my name is Katie Hawkins and I am a Director of Regulatory Affairs in the General Counsel's office at WEX, a global financial services and technology company headquartered in Portland. Thank you for the opportunity to testify today.

WEX has established and adopted comprehensive privacy frameworks which comply with the most stringent global privacy laws passed to date: the General Data Protection Regulation ("GDPR") in Europe, California's Consumer Privacy Act, and the Health Information Portability and Accountability Act, or HIPAA . We support measures that bring similar standards and safeguards to Maine's consumers. And we are encouraged that the Judiciary Committee is focused on bringing greater transparency to consumers around business practices when it comes to their data.

At WEX, we take our duty to protect and secure data seriously. Employers across the country rely on WEX technology to manage the administration of health benefits for their employees; this includes approximately 19.5 million benefits administration accounts. We are keenly aware that our customers and their employees will only trust WEX technology if they know their data is private.

WEX is encouraged by the goal of this bill to enhance consumer privacy and protect personal information. However, we caution the Committee to carefully reconsider and correct four distinct problems with its current form, which would diverge from other privacy laws, complicate enforcement, and significantly detract from the legislation's overall effectiveness.

1) Refine the **definition of "Large Data Holders."** Company size alone does not justify a long list of unnecessary requirements that fail to take into consideration the nature of the business.

Sections 9608, 9611, 9612 and 9617[1] place undue burdens of retaining, reporting, and resourcing privacy compliance programs that go well above current law in states where privacy laws have been passed.

2) **Remove the private right of action.** The bill's private right of action, with no need to prove actual harm, opens the proverbial floodgates to costly, time-consuming, and even trivial litigation for consumers and companies alike. Most jurisdictions that have passed privacy laws reject a private right of action. In Europe, for example, individual complaints are directed to specialist regulatory bodies, rather than the courts. These specialist entities can assess and filter-out meritless claims, investigate only when truly necessary, and work with (not against) companies in giving a complainant an appropriate, proportionate remedy.
3) **Add an exemption for data protected under HIPAA** We recommend that information covered by HIPAA and other similar data already governed by various federal laws be exempt from this legislation. Other states such as Texas, Virginia, Iowa, Montana, and Indiana do this to dispel any uncertainty about whether state or federal law takes precedence.
4) **Extend the implementation period.** Section 9620 provides an effective date of one-hundred and eighty days after adjournment. For WEX, with a large privacy compliance program in place, this is not a problem. But for smaller covered entities and those only operating within Maine, a full year is needed to build one from the ground up[2].

Again, we commend the Judiciary Committee for taking action on this important issue. We welcome a continued dialogue and appreciate the opportunity to be involved. A strong baseline of standards is necessary to give people meaningful protections, and we believe supporting laws like these are good for our customers and important for holding the industry to higher standards. But we caution

---

[1] 9608 requires these holders to *make publicly available* old privacy policies, with detailed histories of their revisions, *for ten years*. It is not at all clear what privacy purpose this serves, nor why such an obligation should fall exclusively on Large Data Holders. Lack of a rational purpose is also seen in s. 9611, requiring large holders to respond to certain individual privacy requests (for example, to delete their data) within forty-five days, compared to sixty days for other covered entities. To further complicate matters, under s. 9612, these larger companies have heavy statistical and reporting obligations, which contribute nothing to the practical, everyday protection of privacy rights. To the contrary, this section only diverts attention and resources away from people and towards "paper compliance" instead. This disconnect between the added burdens on Large Data Holders and their real-world business most clearly appears in s. 9617's mandate that they, unlike other covered entities, appoint a special privacy officer "on steroids," acting as a sort of internal auditor requiring extra (and costly) internal resourcing. Not even California requires this and, while the European Union does, it rightly limits these only to industries having serious, direct impact upon people's privacy, like telecommunications and social media. Company size alone does not matter there, as it does here in LD1977. In this sense, then, the Bill's very definition of "Large Data Holder" is flawed, so that the distinction should be rejected outright

[2] In June 2023, California's Superior Court granted a stay of enforcement of the CPRA for 12 months after the adoption of all regulations required by the CPRA, delaying enforcement until after March 2024.

that these standards must be inline with what can be reasonably achieved by Maine's business community. Aligning this law with those already set forth in other states will minimize the operational burden that could compromise Maine's environment for doing business.