INNOVATIVE PAYMENTS ASSOCIATION

Proposed Framework for Federal Privacy Legislation

Objectives:

- U.S. Leadership as a Champion of Consumer Privacy and Corporate Accountability
- Technology Neutral to Foster Innovation and Competition
- Reduce Regulatory Burdens by Harmonizing Federal and State Laws and Regulations
- Global Protection for U.S. Consumers through Global Interoperability

Framework Core Principles

Covered Organizations and Effect on Other Laws

- Apply a consistent, uniform framework to the collection, use, and sharing of personal data that is not industry specific by harmonizing federal laws and regulations and preempting conflicting state and local laws and regulations—conflicting standards undermine consumer expectations and trust.
- Simultaneously protect consumer privacy and minimize the compliance burdens on small businesses by considering the amount, type, and risk of processing of personal data.
- Remove the obstacles for law enforcement by not interfering with government and law enforcement activities regarding personal data.
- Include common sense exemptions from any requirements to obtain consent for collection, maintenance, use or dissemination of personal information in connection with the following activities:
    - To approve, guarantee, process, administer, complete, enforce or provide any product, service, account, benefit, transaction or payment method that is requested or approved by the individual, or used to deliver goods, services, funds or other consideration to, or on behalf of, an individual;
    - To evaluate, detect or reduce risk, fraud, identity theft or possible criminal activities;
    - To provide fraud and risk scoring services, support research and analytics for developing or enhancing products and services, and performing services to maintain an account.
    - Privacy legislation should include a carve-out for any financial institution subject to the GLBA. The exemptions discussed above should take note that the privacy practices of financial institutions are already governed by the Gramm-Leach-Bliley Act, or GLBA, which broadly applies to any non-public information about an individual that a financial institution collects in connection with a financial service or product. GLBA already imposes a number of requirements on financial institutions with respect to non-public information they collect, including with respect to how such information is shared, used, and maintained.

One Definition of Personal Data

- Personal data should be defined as consumer data that is held by the organization and identifies or is identifiable to a natural, individual person, including but not limited to: name and other identifying information (e.g., government-issued identification numbers), and personal

information derived from a specific device hat reasonably could be used to identify a specific individual.
- De-identified data and certain data in the public domain are exempt.
- Designate categories of sensitive personal data that are subject to additional obligations and protections.

Reduce Compliance Burdens by Leveraging Risk-Based Privacy Practices
- Eliminate specific risk practices established by regulations.
- Organizations should balance the benefits of its personal-data processing activities to itself, individuals, and society against the potential risks and applying appropriate mitigations.
- Mitigate high-risk data processing activities by conducting privacy impact assessments and utilizing robust data protection processes (e.g., de-identification, or encryption).

Individual Rights that Empower Consumers and Protect Organizations' Legitimate Interests
- Transparency. Consumers should have reasonable access to clear and understandable information about: (a) how and why their personal data is being collected, used, and disclosed (and to whom); (b) how to exercise their rights; and (c) who they can contact in the organization for questions regarding data processing activities. Consumer access should be limited to instances where a consumer makes a verifiable request.
- Reasonable Consumer Control. Organizations should be allowed flexibility in determining appropriate consumer controls, considering the sensitivity of the personal data, risk and context of data processing, and sharing of personal data with unaffiliated third parties. Consumers should have the opportunity to choose whether their data may be sold to non-affiliated third parties, and to understand how opting out (withholding consent) may result in the unavailability of certain good and services offered by an organization to that consumer.
- Access and Correction. Consumers, upon making a verifiable request, should have a reasonable right to access and correct any inaccuracies in personal data collected by an organization.
- Deletion. Organizations should be required to comply with a consumer's request to delete the personal data collected by the organization when such data is no longer required to be maintained under applicable law or no longer necessary for the organization's legitimate business purposes.
- Organizations' Legitimate Interests may include protecting the health and safety of individuals, preventing fraud, authenticating an individual and addressing security risks, supporting legitimate scientific and research purposes, and satisfying business and legal obligations.

Governance
- Organizations should develop and implement policies and procedures consistent with the core principles, include data protection obligations in contracts with services providers providing processing services, and establish appropriate mechanisms to address consumer inquiries and complaints regarding the organizations' personal data practices.

Data Security and Breach Notification

- Organizations should implement reasonable and appropriate administrative, technical, and physical safeguards to protect against the unauthorized access to or disclosure of personal data.
- Breach notification requirements should preempt state and local breach notification laws and establish reasonable timeframes for breach notification if there is a reasonable risk of significant harm as a result of a personal data breach.

Enforcement

- No Private Right of Action. Enforcement is best handled by federal regulators and state Attorneys General. A private right of action would create unnecessary and costly litigation.
- The Federal Trade Commission should be the federal agency for enforcement.
- State Attorneys General should be able to bring an enforcement action in federal court on behalf of their state's residents.
- Enforcement actions and fines should consider the following: direct harm caused severity of the harm, an organization's conduct and mitigation steps taken, the degree of intentionality or negligence of an organization, the degree of cooperation, and an organization's prior conduct and history related to the privacy and security of personal data.
- Industry groups should be encouraged to develop Codes of Conduct or Assessments as an alternative method of compliance. Once approved by an appropriate federal agency, an organization's compliance with the appropriate code of conduct or assessment shall create a presumption of compliance with the national privacy law.

INNOVATIVE PAYMENTS ASSOCIATION

APPENDIX—A
TALKING POINTS

One Standard

U.S. companies are currently subject to the specific data privacy laws of each of the 50 states, as well as whatever federal privacy laws may apply to their particular industry and, depending on their operations, the EU's General Data Protection Regulation, or GDPR.

Attempting to comply with these various laws and regulations is extremely difficult and expensive and may have far reaching impacts on interstate commerce. The current patchwork of state privacy laws is made worse by the fact that several states have either recently passed laws (e.g., CA) or have introduced bills (e.g., NY, WA, MA, MD) to further modify their existing data privacy requirements. In the case of California, the state's privacy law has already been amended once and further changes are expected later this year, making it difficult for companies to know what work they should be currently undertaking with respect to their privacy practices in order to comply with developing state law.

A Nationwide Privacy Framework

When it comes to effective privacy protections, consumers and businesses benefit when there is certainty and consistency with regard to laws and regulations. Congress should pass legislation that sets one standard and expressly preempts state law on matters concerning data privacy in order to provide certainty and consistency to consumers and industry. Absent such preemption, there will be market confusion, as companies struggle to comply with a patchwork of differing and potential inconsistent state laws without the benefit of a baseline standard they should be following for privacy. In addition, a patchwork of state laws could deter new entry into the marketplace, as the costs with developing a privacy program that complies with the laws of all 50-states may simply be more than most companies can bear. Thus, the absence of federal legislation harms innovation and competition.

Congress Has Passed Laws with Preemption Provisions

There is precedence for Congress to take action to preempt state law in this area. For example, three federal privacy statutes have preemption provisions: the Children's Online Privacy Protection Act of 1998; the CAN-SPAM Act, passed in 2003, and the 1996 and 2003 updates to the Fair Credit Reporting Act.

Cross-Border Concerns

In May 2018 the GDPR went into effect in the European Union. The GDPR is already having a significant global impact, as companies located around the work struggle to comply with its many restrictive and onerous provisions. If the U.S. continues to operate with a patchwork of various state laws governing data privacy, and not a national standard, it may negatively impact our ability to influence international privacy policy discussions.

DOCS/2231936.3