March 27, 2023

Via electronic mail

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

Re: **Preliminary Comments on Proposed Rulemaking Under the California Consumer Privacy Act (PR 02-2023)**

The Bank Policy Institute[1] appreciates the opportunity to submit preliminary comments to the California Privacy Protection Agency on the proposed rulemaking on cybersecurity audits, risk assessments, and automated decisionmaking under the California Consumer Privacy Act, as amended by the California Privacy Rights Act.[2]

I. Executive Summary

BPI's members are financial institutions that have invested significant time and resources into building data protection and information security compliance systems that align with federal and state financial privacy, consumer protection, and other financial services laws. BPI members are committed to promoting robust privacy protections for California consumers. Drawing on the experience of its members operationalizing privacy and security safeguards for their customers, BPI has provided comments on each of the three areas that will be addressed in the forthcoming rulemaking: cyber audits, risk assessments, and automated decisionmaking.[3] In particular, BPI urges the Agency to consider:

- Exempting federally-regulated financial institutions from any new audit, risk assessment, and automated decisionmaking requirements, to avoid duplication, conflict, or interference with the existing financial services regulatory scheme;

- Specifying, at a minimum, that financial institutions' existing auditing and risk assessment activities satisfy any new regulatory requirements and are not required to be disclosed to the Agency;

---

[1] The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost two million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

[2] Cal. Civ. Code § 1798.100 *et seq.*

[3] While BPI has provided its responses in a narrative form, it has listed the relevant questions addressed in its comments at the start of each section below.

- Harmonizing any new requirements with existing banking regulation and supervision in these areas, as well as with similar audit and risk assessment provisions in the U.S. and international jurisdictions and other consumer protection and privacy frameworks; and

- Creating necessary exemptions for opt-out and access rights for automated decisionmaking, including where there is the involvement of a human in decisionmaking, where the outcome does not result in legal or similar detriment to the consumer, for automation that is used in furtherance of regulatory compliance goals or for security and fraud-prevention purposes, and for trade secrets.

The regulations should recognize the paramount role that financial regulators play in regulating national and state banks and savings associations and their affiliates.[4] These institutions already are subject to robust regulation and active supervision in these three areas, including by federal prudential regulators (i.e., Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency) and, for state-chartered financial institutions, state banking regulators. [5] Information security and use of artificial intelligence are evaluated as part of financial regulators' comprehensive and ongoing supervision of banks' risk management systems and compliance with applicable laws and regulations. Federal supervision requires that all banks have internal controls and information systems that are appropriate to the size of the institution and the nature, scope, and risk of its activities. Banks are also required to have an internal audit system appropriate to the nature and scope of a bank's activities and that is informed by a risk assessment process.

The CCPA statute exempts many federally-regulated financial institution activities because it explicitly exempts personal information subject to the Gramm Leach Bliley Act.[6] However, most of the regulatory frameworks and requirements discussed in this letter apply broadly to all information assets of an institution – not just those that are subject to the GLBA.[7] Thus, the Agency should expressly exempt federally-regulated financial institutions from any new audit, risk assessment, and automated

---

[4] For purposes of this letter, BPI uses the term "federally-regulated financial institutions" to refer to entities regulated by the federal prudential regulators, *i.e.*, the Board, FDIC, and OCC, (collectively, referred to as "banks") and their affiliates. Both terms encompass state banks that are chartered at the state level, as such banks remain subject to supervision and examination by federal prudential regulators – the Federal Reserve in the case of banks that have joined the Federal Reserve System, and the FDIC in the case of other state-chartered banks.

[5] In addition, the National Credit Union Administration, Securities and Exchange Commission, Commodity Futures Trading Commission, Federal Trade Commission, Consumer Financial Protection Bureau, and the Federal Housing Finance Agency all have regulatory, supervisory, enforcement, and/or examination authority over cybersecurity matters with respect to entities within their jurisdiction. Other regulatory bodies include individual state banking, insurance, and securities regulators as well as non-governmental self-regulatory organizations, such as the Financial Industry Regulatory Authority, National Futures Association, and the Municipal Securities Rulemaking Board.

[6] The CCPA exempts information collected, processed, sold, or disclosed subject to the GLBA and implementing regulations or the California Financial Information Privacy Act. *See* Cal. Civ. Code § 1798.145(e).

[7] *See, e.g.,* FFIEC, IT EXAMINATION HANDBOOK: INFORMATION SECURITY, at 1 (Sept. 2016), https://ithandbook.ffiec.gov/media/274793/ffiec_itbooklet_informationsecurity.pdf ("Information Security Booklet") (noting that the booklet "addresses regulatory expectations regarding the security of all information systems and information maintained by or on behalf of a financial institution"); 12 C.F.R. § 30, Appendix A (OCC) ("OCC Interagency Guidelines Establishing Standards for Safety and Soundness"); 12 C.F.R. § 208, Appendix D-1 (Board); and 12 C.F.R. § 364, Appendix A (FDIC).

decisionmaking requirements to avoid any duplication, conflict, and interference with existing financial services regulatory schemes.[8]

In particular, for national banks and federal savings associations, visitorial rights restrict the ability of states to inspect, examine, or regulate these entities' activities that are authorized under federal banking law.[9] There would be serious questions about the permissibility of state requirements to conduct – and, certainly, to share with state privacy regulators – audits and risk assessments that involve the processing of personal information in connection with activities that affect lending, deposit taking, and other national bank and federal savings association operations. It is thus crucial that banks and savings associations are exempt from any new audit and risk assessment requirements and any expectations to make such materials available to California regulators.

In addition, to the extent that any federally-regulated financial institutions are not categorically exempt from the substantive audit and risk assessment requirements, the Agency should harmonize any new requirements with existing banking regulation and supervision in these areas, as well as with similar audit and risk assessment requirements in the U.S. and international jurisdictions such as Europe and the United Kingdom.

Similarly, any new California privacy requirements related to automated decisionmaking should not be applied to federally-regulated financial institutions to avoid disrupting or interfering with existing financial regulation and supervision. At a minimum, the Agency should be careful not to limit the ability of banks to use automation in various ways that further important public policy interests, such as security and prevention of fraud and other financial crimes. To the extent federally-regulated financial institutions are not exempted, any applicable requirements should be interoperable with other consumer protection and privacy frameworks.

II. Cybersecurity Audits

- *What laws that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require cybersecurity audits?*
- *What would the benefits and drawbacks be for businesses and consumers if the Agency accepted cybersecurity audits that the business completed to comply with the laws identified in question 1,*

[8] The Agency clearly has the authority to exempt these industries, as the statute does not compel implementation of new requirements in industries or contexts where the record does not support it. Moreover, the CCPA should not restrict a business's ability to comply with federal laws, Cal. Civ. Code § 1798.145(a)(1), or conflict with federal law, *id.* § 1798.196.

[9] *See* 12 U.S.C. § 484 ("No national bank shall be subject to any visitorial powers except as authorized by Federal law, vested in the courts of justice or such as shall be, or have been exercised or directed by Congress or by either House thereof or by any committee of Congress or of either House duly authorized."). Visitorial powers are defined as (i) examination of a bank; (ii) inspection of a bank's books and records; (iii) regulation and supervision of activities authorized or permitted pursuant to federal banking law; and (iv) enforcing compliance with any applicable federal or state laws concerning those activities. Notably, examination of a bank's books and records is not limited to on-site inspection. *See* 12 C.F.R. § 7.4000; *see also Watters v. Wachovia Bank, N.A.*, 550 U.S. 1, 21 (2007) ("[S]tate regulators cannot interfere with the 'business of banking' by subjecting national banks or their OCC-licensed operating subsidiaries to multiple audits and surveillance under rival oversight regimes."). These requirements have been explicitly extended to federal savings associations and their subsidiaries. *See* 12 CFR § 7.4010(b).

or if the Agency accepted any of the other cybersecurity audits, assessments, or evaluations identified in question 2?

- *With respect to the laws, cybersecurity audits, assessments, or evaluations identified in response to questions 1 and/or 2, what processes help to ensure that these audits, assessments, or evaluations are thorough and independent?*

As part of the robust regulation described above, banks are already subject to comprehensive cybersecurity auditing requirements, including obligations to maintain their own audit programs and, significantly, on-site examinations by their prudential regulators that cover cybersecurity. Accordingly, federally-regulated financial institutions should be exempted from any cybersecurity audit regulations promulgated by the Agency or, in the alternative, permitted to rely on their existing cybersecurity audits. As discussed above, an exemption also helps avoid raising potential inconsistencies with visitorial powers for national banks and federal savings associations.

A number of federal financial services laws and regulations require banks and other financial institutions to manage cyber risks, including through an appropriate audit program. These include but are not limited to the information security provisions of GLBA and its implementing regulations and guidance.[10] For example, GLBA regulations require banks to not just maintain an information security program, but to regularly monitor, evaluate, and adjust their information security program in light of internal and external threats and other factors.[11] As a practical and administrative matter, the information security programs are necessarily designed to cover and protect all of a bank's information assets, and not just personal data subject to GLBA. Moreover, banks are also subject to general "safety and soundness" requirements, under which banks are required to maintain internal controls, information systems, and an internal audit system that are appropriate to the size of the institution and the nature, scope, and risk of its activities.[12]

Building on these legal obligations, the federal prudential regulators have developed an extensive inventory of policy statements, toolkits, and other guidance that set regulatory expectations for banks' information security programs. Among other requirements, a bank's information security program should be tested and evaluated through internal audits, self-assessments, and tests.[13] Moreover, perhaps uniquely among other industries, external bank examiners from the federal prudential regulators regularly examine the adequacy of bank information security programs, information systems, and audit programs – along with other topics – based on standards set forth in the Federal Financial Institutions Examination

---

[10] *See* 15 U.S.C. § 6801(b); 12 C.F.R. § 30, Appendix B (OCC) ("OCC Interagency Guidelines Establishing Information Security Standards"); 12 C.F.R. § 208, Appendix D-2 and § 225, Appendix F (Board); and 12 C.F.R. § 364, Appendix B (FDIC).

[11] *See, e.g.,* OCC Interagency Guidelines Establishing Information Security Standards at Sections II, III.

[12] 12 U.S.C. §§ 1818, 1831p-1; OCC Interagency Guidelines Establishing Standards for Safety and Soundness; 12 C.F.R. § 208, Appendix D-1 (Board); and 12 C.F.R. § 364, Appendix A (FDIC).

[13] *See* Information Security Booklet at 53; *see also* OCC, COMPTROLLER'S HANDBOOK: INTERNAL AND EXTERNAL AUDITS, at 2 (July 2019), https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/internal-external-audits/pub-ch-audits.pdf ("Comptroller's Handbook"); OCC Bulletin 2003-12: Interagency Policy Statement on Internet Audit and Internal Audit Outsourcing; OCC Bulletin 99-37: Interagency Policy Statement on External Auditing Programs; and FFIEC, IT EXAMINATION HANDBOOK: AUDIT (April 2012), at A-1–A-17, https://ithandbook.ffiec.gov/media/274709/ffiec_itbooklet_audit.pdf ("Audit Booklet").

Council's Information Technology Examination Handbook ("IT Handbook").[14] These examiners will assign a rating to the bank, identify deficiencies that must be remedied, work with management to obtain corrective action, and pursue enforcement related to their findings as necessary.[15]

Financial institutions also need to navigate a broader cyber regulatory environment. State financial regulators in some jurisdictions have set out robust requirements that state-chartered banks maintain a cybersecurity program that is based on a risk assessment and tested and audited.[16] Among them, the New York Department of Financial Services has robust requirements that mandate annual certifications of compliance.[17] As another example, broker dealers and others within the jurisdiction of the Securities and Exchange Commission are subject to a separate set of information security rules, which the SEC currently is in the process of strengthening.[18]

a) Bank Audit Programs

As noted above, banks are expected to maintain an effective information security program that is tested through an internal audit program that is appropriate to the size and complexity of the institution.[19]

Under interagency guidelines, as part of its information security program, a financial institution must conduct cybersecurity audits and risks assessments to determine foreseeable risks and threats, both internal and external, to the security, confidentiality, and integrity of customer information. For example:

- Conducting periodic reviews of access controls;
- Inventorying data, systems, applications, devices, platforms, and personnel;
- Ensuring customer information is encrypted at-rest and in-transit;

[14] The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve, FDIC, OCCCFPB and NCUA. *See* FFIEC, Homepage, https://www.ffiec.gov/ (last accessed March 15, 2023).

[15] *See, e.g.,* Information Security Booklet at 74; 12 U.S.C. § 1818(b) (outlining procedure for a cease-and-desist order to issue against a bank if its prudential regulator believes that it is engaging or has engaged, or has reasonable cause to believe that it is about to engage, in an unsafe or unsound practice or violation of a law, rule, regulation, or condition imposed in writing upon the bank by the regulator).

[16] *See, e.g.,* 23 NYCRR § 500 (setting out robust cybersecurity requirements, including risk assessments).

[17] *See id.*

[18] *See* 17 C.F.R. § 248.30 (Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information); SEC, SEC Proposes Changes to Reg S-P to Enhance Protection of Customer Information, https://www.sec.gov/news/press-release/2023-51 (March 15, 2023). *See also* 16 C.F.R. § 314 (setting out information security requirements for financial institutions subject to the FTC's GLBA jurisdiction, including risk assessment requirements).

[19] *See, e.g.,* Information Security Booklet at 53; Audit Booklet at 1; and OCC Interagency Guidelines Establishing Information Security Standards at Sections II, III.

- Identifying and assessing the risks to customer information in each relevant area of a company's operation, such as with respect to service providers and changes in the firm's operations;

- Managing and controlling risk, including regularly testing key controls, systems, and procedures of the information security program. Tests must be conducted or reviewed by independent third parties or independent staff;

- Overseeing service provider arrangements, including conducting due diligence and reviewing audits, risk assessments, and tests of service providers and their information security programs;

- Implementing a program to respond to and mitigate data breaches involving customer data, including providing federal regulators, relevant law enforcement, and consumers notification of breaches; and

- Providing at least annually a report to the board or an appropriate committee of the board the overall status of the information security program and compliance with relevant regulations.[20]

To assist with self-assessments, the prudential regulators have developed a Cybersecurity Assessment Tool for banks to use to evaluate their cyber maturity that is consistent with and provides mapping to the National Institute of Standards and Technology Cybersecurity Framework (along with mapping to the FFIEC IT Handbook).[21]

In respect of a more formal cybersecurity audit program, banks are expected to maintain an audit program that is appropriate to the size and complexity of the institution.[22] These programs must meet specific requirements, such as the adequate monitoring of the system of internal controls through an internal audit function, independence and objectivity, qualified persons, and adequate testing and review of information systems.[23] Most large banks are also subject to the OCC's supplemental requirements referred to as "heightened standards."[24]

---

[20] *See, e.g.,* OCC Interagency Guidelines Establishing Information Security Standards at Section III; Comptroller's Handbook at 22.

[21] *See* FFIEC, CYBERSECURITY ASSESSMENT TOOL (May 2017), https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf. NIST's Cybersecurity Framework is well-aligned with the processes and goals articulated in the CCPA. Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* made the NIST Cybersecurity Framework mandatory for all US federal government agencies. The NIST Cybersecurity Framework was designed specifically for companies that are part of the US critical infrastructure. As a comprehensive framework, the NIST Cybersecurity Framework provides industry standards, guidelines, and practices that allow for communication of cybersecurity activities and outcomes across an organization from the executive level to the implementation and operations levels.

[22] *See, e.g.,* OCC Interagency Guidelines Establishing Information Security Standards at Section II.B (requiring "an internal audit system that is appropriate to the size of the institution and the nature and scope of its activities").

[23] *See, e.g., id.* They also must be independent; for example, other OCC guidance suggests that "[b]ank audit programs must be performed by independent and competent staff who are objective in evaluating the bank's control environment." Comptroller's Handbook at 2.

[24] *See* 12 C.F.R. § 30, Appendix D. For example, large OCC-regulated banks are, among other requirements, required to maintain a complete and current inventory of all material processes, product lines, services, and

Together, these audit program requirements address the management of cyber risks broadly and go beyond consumer personal information.[25] Further, banks are directed to use an industry cybersecurity control framework, such as the NIST Cybersecurity Framework or Committee of Sponsoring Organizations of the Treadway Commission framework, as the basis for audit scope and objective.[26] As a practical matter, banks also must assess their information program against the FFIEC IT Handbook standards against which banks are examined by their regulators.

Finally, banks are examined by their regulators for the adequacy of their audit programs. Examiners will assess the qualifications of the IT audit staff, quality of the audit, and level of audit independence.[27] The assessment includes some level of audit validation, including verification procedures as necessary, and examiners may expand their supervisory activities if they identify concerns with the internal audit.[28]

b) FFIEC IT Examinations

Banks (and their technology service providers) are also subject to direct examination by the federal prudential regulators on their information security programs pursuant to the FFIEC examination standards.[29] These exams cover, for example, information security program governance and management; information security policies, standards and procedures; classification of technology assets; user security controls; and other topics, as set forth in the IT Handbook.[30] Further, examiners may conduct on site-reviews, including independent testing of the bank's cybersecurity, such as through penetration testing. Examiners then prepare an examination report, assign ratings to the bank's activities, and identify any deficiencies that must be remedied by the bank.[31] These examiners will work with management to obtain corrective action, but the regulators can also pursue enforcement related to deficiencies.[32] Federal

---

functions and assess the risks associated with each; establish and adhere to an audit plan that is periodically reviewed and updated; establish and adhere to processes for independently assessing the design and ongoing effectiveness of the risk governance framework on at least an annual basis; and establish a quality assurance program that ensures internal audit's policies, procedures, and processes comply with applicable regulatory and industry guidance, are appropriate for the size, complexity, and risk profile of the covered bank, are updated to reflect changes to internal and external risk factors, emerging risks, and improvements in industry internal audit practices, and are consistently followed. *Id.* at II.C.3.

[25] *See, e.g.,* OCC Interagency Guidelines Establishing Standards for Safety and Soundness (placing no restrictions on the scope of the required audits); 12 U.S.C. § 1831p-1 (requiring the federal banking agencies to prescribe standards relating "internal controls, information systems, and internal audit systems" with no limitation to consumer personal information).

[26] *See, e.g.,* Comptroller's Handbook at 112.

[27] *See* Audit Booklet at A-1–A-17.

[28] *See, e.g.,* Comptroller's Handbook at 2.

[29] *See* Information Security Booklet (provides guidance to examiners and addresses how examiners evaluate information security risks); FFIEC, SUPERVISION OF TECHNOLOGY SERVICE PROVIDERS (Oct. 2012), https://ithandbook.ffiec.gov/media/274876/ffiec_itbooklet_supervisionoftechnologyserviceproviders.pdf.

[30] *See* Information Security Booklet.

[31] *See, e.g., id.* at 74; Comptroller's Handbook at 70.

[32] *See, e.g.,* 12 U.S.C. § 1818(b).

financial regulators are thus heavily involved in both assessing a bank's internal audits and in conducting their own examinations, and may require banks to address any deficiencies that are identified through these internal and external audits.

c) Recommendations: Exemption & Interoperability

To sum, banks are subject to extensive auditing for cyber security and are examined by prudential regulators with expertise pertinent to this highly-regulated industry. Under the existing federal standards, banks already perform cybersecurity audits in any scenario where processing might present "significant risk" to consumers' privacy or security. They also perform cybersecurity audits even where such "significant risks" are not present. Further, these audits clearly meet the "thorough and independent" standard set forth in California law.[33]

For banks, any new cybersecurity audit requirement would at best be duplicative of, and at worst conflict with, the comprehensive and robust financial regulatory frameworks governing information security and cyber security audits for banks. For national banks and federal savings associations, such requirements would raise serious questions with respect to the OCC's exclusive visitorial powers. More generally, such application would frustrate federal policy goals: as noted in the FFIEC's authorizing statute, the FFIEC was created with the goal to "promote consistency in such examination and to insure progressive and vigilant supervision."[34] It also would not be consistent with the statutory design of the CCPA, which sought to avoid interference with federal regulation.[35] Finally, new cybersecurity audit requirements would be duplicative without adding any value for consumers.

BPI therefore urges that the Agency exempt federally-regulated financial institutions from any new cyber audit requirements. At a minimum, it should be clear that such institutions' existing auditing and information security activities satisfy any new regulatory requirements, although such audits must remain internal and should not be accessible to state privacy regulators. For similar reasons, the Agency should provide flexibility to conduct audits using an internal audit team. In no circumstances should such audits be made public. These audits contain highly sensitive information that, if compromised, could increase cyber risk for the banking system. Indeed, such institutions themselves are prohibited by law from disclosing the results of bank examinations performed by financial regulators as confidential supervisory information.[36]

III. Risk Assessments

- *What laws or other requirements that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require risk assessments?*
- *What would the benefits and drawbacks be of the Agency following the approach outlined in the European Data Protection Board's Guidelines on Data Protection Impact Assessment?*
- *What would the benefits and drawbacks be if the Agency considered the data protection impact assessment content requirements under GDPR and the Colorado Privacy Act?*
- *In what format should businesses submit risk assessments to the Agency?*

---

[33] Cal. Civ. Code § 1798.185(a)(15)(A).

[34] 12 U.S.C. § 3301.

[35] Cal. Civ. Code §§ 1798.145(a)(1), 1798.145(e).

[36] *See, e.g.,* OCC Bulletin 19-15: Supervisory Ratings and Other Nonpublic OCC Information: Statement on Confidentiality.

As part of the regime described above, banks are also required to conduct risk assessments in relation to processing activities involving personal information. In addition, the OCC's visitorial rights restrict the ability of states to inspect or examine national banks and federal savings associations for processing activities authorized under federal banking law. Thus, federally-regulated financial institutions (and, in particular, national banks and federal savings associations) should be exempted from any risk assessment regulations promulgated by the Agency. In any event, BPI supports regulations that are interoperable with the requirements for data protection assessments under the General Data Protection Regulation, other state privacy laws, and self-regulatory standards, and include sufficient protections for the confidentiality of these audits, as described further below.

a. Existing Risk Assessment Obligations

Banks are subject to risk assessment requirements as part of their information security program. For example, under the GLBA framework, banks must identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems, assess the likelihood of damage from these threats, and assess the sufficiency of policies, procedures and other measures to control these risks.[37] In addition, the FFIEC examination standards require a "risk assessment process to describe and analyze the risks inherent in a given line of business" that occurs at least annually.[38] This process is conducted prior to banks' internal audits, in an effort to "document a bank's significant business activities and associated risks" to prioritize the allocation of audit resources.[39] And, separately, financial institutions also must have identity theft prevention programs under the Fair Credit Reporting Act, which involve the identification of red flags for identity theft and protocols to address identity theft.[40] While these regimes also have broader goals, they serve in part to regulate and supervise banks' use and implementation of risk assessments in these areas.

b. Recommendations: Exemption & Interoperability

BPI strongly urges the Agency to either provide a categorical exemption from any new risk assessment requirements for federally-regulated financial institutions, or to specify that risk assessments that are conducted pursuant to other international, federal, or state privacy or banking laws or regulations satisfy any expectations for risk assessments in California and do not need to be provided to the California regulators.

BPI further urges the Agency to make any rules on risk assessments interoperable with the requirements for data protection assessments under the GDPR, the other state privacy laws, and self-regulatory standards. The European Data Protection Board's *Guidelines on Data Protection Impact Assessment* ("EDPB Guidelines") appropriately focuses resources on risk assessments where there is a

---

[37] *See, e.g.,* OCC Information Security Standards at Part III.B.

[38] Audit Booklet at 8.

[39] *See, e.g.,* Comptroller's Handbook at 23–26 (outlining OCC's audit risk assessment methodology and requirements).

[40] *See, e.g.,* 12 C.F.R. § 41, Subpart J (Red Flags Rule).

higher risk of harm to consumers.[41] In particular, the standard in the EDPB Guidelines requires an assessment where processing is "likely to result in a high risk."[42] Similarly, some other state privacy laws require assessments for "processing activities that present a heightened risk of harm to consumers[.]"[43] Likewise, California should focus its requirements on where there is likely to be a high or heightened risk of harm to consumers, in line with the "significant risk" standard in the statute.[44] Further, it should be clear that these assessments only apply to processing activities that are commenced prospectively.

c. Confidentiality Issues

If banks are not categorically exempt from risk assessment obligations, then they should nonetheless be exempt from any obligation to share these assessments with the Agency given the existing oversight of prudential regulators and the importance of protecting confidentiality. On this point, BPI notes that the GPDR only requires prior consultation with data protection authorities in limited circumstances.[45]

The regulations should also specify, as do other state privacy laws, that the assessments are confidential and exempt from public inspection and copying, and that the disclosure of a risk assessment does not constitute a waiver of any attorney-client privilege or work-product protection that otherwise might exist with respect to the assessment.[46] This final requirement is necessary to avoid suppressing the ability of businesses to obtain legal counsel related to potential privacy risks and safeguards. However, it is equally important to preserve general confidentiality from the public, as risk assessments conducted by financial institutions may contain highly sensitive information that could increase cybersecurity risks, harm consumers, and undermine the safety and soundness of financial institutions. Financial institutions themselves are prohibited by law from disclosing the results of bank examination, as well as other materials prepared for use by supervisors, as confidential supervisory information. This information is also protected from disclosure under the Freedom of Information Act.[47]

To sum, the Agency should exercise this opportunity to set the precedent now for interoperability across regimes and protection of confidential and privileged information.

IV. Automated Decisionmaking

- *What laws requiring access and/or opt-out rights in the context of automated decisionmaking currently apply to businesses or organizations (individually or as members of specific sectors)?*
- *How have businesses or organizations been using automated decisionmaking technologies, including algorithms? In what contexts are they deploying them?*

---

[41] *See* EUROPEAN DATA PROTECTION BOARD, GUIDELINES ON DATA PROTECTION IMPACT ASSESSMENT (DPIA) AND DETERMINING WHETHER PROCESSING IS "LIKELY TO RESULT IN A HIGH RISK" FOR THE PURPOSES OF REGULATION 2016/679 (April 4, 2017), *available at* https://ec.europa.eu/newsroom/article29/items/611236.

[42] *Id.* at 8–14.

[43] Va. Code Ann. § 59.1-576(A)(5); *see also* Colo. Rev. Stat. § 6-1-1309(1).

[44] Cal. Civ. Code § 1798.185(a)(15).

[45] Regulation 2016/679, OJ L 119/1, Art. 36.

[46] *See* Colo. Rev. Stat. § 6-1-1309(4); Va. Code Ann. § 59.1-576(C).

[47] *See* 5 U.S.C. § 552(b)(8).

The financial services industry is subject to federal laws and regulations that prohibit discrimination and provide transparency and accountability in the use of automated decisionmaking and artificial intelligence, including for employment purposes and extending credit, marketing, and other financial services. These legal requirements mitigate and protect against the same underlying concerns about discrimination and transparency as the CCPA's automated decisionmaking provisions, making additional regulation of federally-regulated financial institution's automated decisionmaking processes unnecessary. At a minimum, however, the Agency should ensure that the rules are interoperable with existing frameworks and narrowly circumscribed, to ensure that they do not restrict banks' ability to use automation for important public policy purposes.

a. Existing Protections

Banks and other financial institutions are subject to a number of additional laws, regulations, and guidance that promote accountability and accuracy in automated decisionmaking. Among them, the Equal Credit Opportunity Act and Regulation B prohibit unlawful discrimination against protected classes in "any aspect of" credit transactions, including through automation.[48] ECOA and Regulation B also provide certain data access rights. These include a right to a statement of reasons for a creditor taking adverse action, including reasons based on automated decisionmaking tools, and a copy of any written appraisals and valuations for certain mortgage loan applications.[49] Automated decisionmaking technologies that produce outcomes with legal or similarly significant effects on an individual (e.g., the denial or provision of financial and lending services) may be subject to these provisions or to provisions of the Fair Credit Reporting Act.[50] Further, the federal Fair Housing Act prohibits discrimination in the sale or rental of housing, residential real estate transactions, or the provision of real estate brokerage services,[51] and Title VII, the Civil Rights Act of 1964, and the Age Discrimination in Employment Act of 1967 protect employees and job applicants from discrimination.[52]

In addition, the Dodd-Frank Wall Street Reform and Consumer Protection Act prohibits unfair, deceptive, or abusive acts or practices ("UDAAP"), and the Federal Trade Commission Act prohibits unfair or deceptive acts or practices ("UDAP").[53] Prohibited UDAAP/UDAPs could include, for example, making false representations to customers about the use of automated technologies in processing customer data or deploying automated technologies in a way that harms customers. These laws are enforced against banks by the Consumer Financial Protection Bureau and the federal prudential regulators.

---

[48] *See* 15 U.S.C. § 1691 *et seq.*; 12 C.F.R. § 1002.

[49] *See* 15 U.S.C. § 1691(d), (e); 12 C.F.R. §§ 1002.9(b)(2) and .14; *see also* CFPB, Consumer Financial Protection Circular 2022-03 (addressing adverse action notice requirements in connection with credit decisions based on complex algorithms).

[50] *See 15 U.S.C. §§ 1681 et seq.*

[51] *See* 42 U.S.C. § 3601 *et seq*.

[52] *See* 42 U.S.C. § 2000e *et seq*. (prohibiting employment discrimination based on race, color, religion, sex and national origin); 29 U.S.C. § 621 *et seq.* (prohibiting employment discrimination against persons 40 years of age or older).

[53] *See* 12 U.S.C. § 5531; 15 U.S.C. § 45.

Further, banks are required to comply with regulatory requirements governing their use of models.[54] Consequently, banks review the models that underlie automated technologies closely, including to monitor model performance, adjust or revise models over time, and supplement model results with other analysis and information as needed.[55] Federal regulators also continue to monitor financial institutions' use of artificial intelligence as part of ongoing risk-based supervision, with an eye towards ensuring that financial institutions use automation in a "safe and sound manner" and in compliance with applicable laws and regulations.[56] The financial regulatory agencies have specifically indicated that they will review banks' use of automated data in credit underwriting, and that they expect robust compliance management of consumer compliance risk, including appropriate testing, monitoring and controls.[57] Thus, the federal financial regulators have made clear that they will continue to address banks' use of automated decisionmaking as needed.

b. Recommendations: Exemption & Interoperability

In order to avoid duplication and ambiguity related to these existing requirements, BPI urges the Agency to exempt federally-regulated financial institutions from the CCPA's requirements related to profiling and automated decisionmaking. In the alternative, it is important that the rules be interoperable with the existing framework and narrowly circumscribed, so that they do not inadvertently restrict banks and other financial institutions' ability to use automation for important public policy purposes.[58]

Among other important limits: such rules should make clear that any new opt out rights do not extend either where (1) there is the involvement of a human in decisionmaking, or (2) the outcome does not result in legal or other similar detriment to the consumer.[59] In addition, there should be an exemption for automation that is used in furtherance of regulatory compliance goals or for security and fraud-

---

[54] *See* OCC Bulletin 11-12: Supervisory Guidance on Model Risk Management; Board SR Letter 11-7: Guidance on Model Risk Management.

[55] *See* OCC Bulletin 11-12 at 4.

[56] *See* OCC et al., Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, including Machine Learning, 86 Fed. Reg. 16837, 16840 (March 31, 2021), https://www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence; Testimony of Kevin Greenfield, Deputy Comptroller for Operational Risk Policy, OCC, before the Task Force on Artificial Intelligence, U.S. House of Representatives Committee on Financial Services.

[57] BOARD, CFPB, FDIC, NCUA, AND OCC, INTERAGENCY STATEMENT ON THE USE OF ALTERNATIVE DATA IN CREDIT UNDERWRITING (2019), https://www.occ.gov/news-issuances/news-releases/2019/nr-ia-2019-142a.pdf.

[58] The Agency should be aware of both the requirements described above and of other emerging voluntary frameworks that banks and other institutions may look toward, such as the new NIST AI Framework, which includes guidance on explainability, transparency, and trustworthiness. *See* NIST, ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK (AI RMF 1.0), at 12–17 and 29–30 (Jan. 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[59] This would mirror the GDPR, as well as aligning with other state privacy laws that restrict only profiling "in furtherance of decisions that produce legal or similarly significant effects concerning the consumer." Va. Code Ann. § 59.1-473(A)(5); Colo. Rev. Stat. § 6-1-1306(1)(a)(I)(c).

prevention purposes by financial institutions and their service providers.[60] There should also be an explicit exemption from any access requirements for a business's trade secrets, confidential or proprietary information, or any other intellectual property or corporate or technological information that is confidential, proprietary, or otherwise restricted from public disclosure.

A contrary result could limit the ability of banks and other financial institutions to use automation in various ways that further important public policy goals, including to detect suspicious transactions and fight against financial crimes, such as fraud, bribery, money laundering, and terrorist financing.[61] For example, banks use automation to identify and report identity theft and suspicious money laundering and terrorist financing activities; prevent parties that are subject to economic sanctions from accessing the U.S. banking system; review payment card transactions to identify and prevent fraud and complete chargebacks for challenged transactions; apply lending standards; and alert customers to account overdraft risk. Banks may also use artificial intelligence to increase access to credit for those who may not be able to obtain credit in the mainstream credit system, as well as to generally increase efficiency, such as in processing of ACH transactions or credit applications, and thus lower costs for consumers.[62] Automated decisionmaking is essential to these activities, given the vast universe of payment and customer data at issue.

*****

The Bank Policy Institute appreciates the opportunity to submit these preliminary comments to the California Privacy Protection Agency on the proposed rulemaking on cybersecurity audits, risk assessments, and automated decisionmaking under the California Consumer Privacy Act, as amended by the California Privacy Rights Act. If you have any questions, please contact the undersigned by phone at (202) 589-1935 or by email at Tabitha.Edgens@BPI.com

Respectfully submitted,

/s/ Tabitha Edgens

Tabitha Edgens
Senior Vice President
Senior Associate General Counsel
Bank Policy Institute

---

[60] The Agency could consider building on existing language in the state privacy laws for this exemption, such as: "A business shall not be required to honor the rights addressed in this subsection if doing so would restrict the business's ability to prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action." *See* Va. Code Ann. § 59.1-578(A)(7); *see also* Cal. Civ. Code § 1798.140(ac).

[61] *See, e.g.,* 31 U.S.C. § 5311 *et seq.*; 12 U.S.C. § 95 and 50 U.S.C. § 4301 *et seq.*; 50 U.S.C. § 1701; and 18 U.S.C. §§ 1956, 1957. These activities are often expressly sanctioned and expected by the banking regulators. *See* BOARD ET AL., JOINT STATEMENT ON INNOVATIVE EFFORTS TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING (2018), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20181203a1.pdf.

[62] *See* BOARD, CFPB, FDIC, NCUA, AND OCC, INTERAGENCY STATEMENT ON THE USE OF ALTERNATIVE DATA IN CREDIT UNDERWRITING (2019).