BUDGETURA™

Regulatory Compliance Framework:

Federal and State Requirements

December 4, 2024

Table Of Contents

Click the titles to jump to that page of the document.

General Overview

Budgetura faces **18 distinct regulatory frameworks** across federal financial privacy, state data protection, communications law, AI/consumer protection, and marketplace regulations. **GLBA likely applies** as a fintech data aggregator, triggering mandatory written security programs and encryption requirements. However, **SEC investment adviser registration is NOT required**—debt payoff advice does not constitute securities advice. The primary compliance risks concentrate in three areas: financial data security under GLBA's 2023 Safeguards Rule, state privacy law patchwork (with Minnesota's July 2025 law notably lacking a GLBA exemption), and CFPB UDAAP enforcement for AI-generated recommendations where "there is no AI exemption" per Director Chopra.

GLBA applies to fintech data aggregators using Plaid

The Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801-6809) **likely covers Budgetura** based on the "financial institution" definition at 16 CFR § 313.3(k). The FTC's Safeguards Rule explicitly lists "credit counselors and other financial advisors" as covered entities, and Budgetura's AI-powered personalized debt recommendations constitute financial advisory services. The determination hinges on activities, not labels—a debt management app accessing consumer bank data through Plaid to provide financial analysis qualifies under the "significantly engaged" standard.

The **2023 Safeguards Rule** (effective June 9, 2023, with breach notification effective May 13, 2024) mandates nine elements for any written Information Security Program: designation of a Qualified Individual, written risk assessments, **mandatory encryption** at rest and in transit, multi-factor authentication for accessing customer information, penetration testing annually plus vulnerability assessments every six months, security awareness training, service provider oversight with contractual security requirements, documented incident response plans, and annual written board reports. Companies with fewer than **5,000 consumers** are exempt from certain procedural elements but core security obligations remain.

Breach notification to the FTC within 30 days is required when unencrypted customer information of 500+ consumers is compromised. Penalties reach **$100,000 per violation** for institutions and **$10,000 per violation** for officers personally, with criminal penalties up to 10 years imprisonment for patterns involving $100,000+ in illegal activity.

The **Privacy Rule** (16 CFR Part 313) requires initial privacy notices at customer relationship establishment, annual notices (with FAST Act exemption if practices unchanged), and opt-out rights before sharing nonpublic personal information with non-affiliates. Sharing with service providers like Plaid under contractual confidentiality agreements is permitted without opt-out.

Implementation requirements: Designate a Qualified Individual (can be external consultant, ~$5,000-15,000 annually), complete written risk assessment within 90 days, implement encryption for all customer data, deploy MFA for administrative access, create incident response plan with clear roles and 30-day notification capability, conduct penetration testing annually, and document data inventory showing what information is stored and where.

State privacy law compliance requires a multi-jurisdictional approach

CCPA/CPRA (Cal. Civ. Code §§ 1798.100-1798.199.100) applies when a business exceeds **$26,625,000 revenue** (2025 CPI-adjusted threshold), processes data of **100,000+ California consumers** (including website visitors tracked via cookies), or derives 50%+ revenue from selling/sharing data. For startups below thresholds, CCPA doesn't formally apply, but the **private right of action for data breaches** (Section 1798.150) applies even to GLBA-covered entities—financial institutions are not exempt from breach-related lawsuits with statutory damages of **$107-799 per consumer per incident**.

The GLBA exemption in CCPA is **data-level, not entity-level**: financial information collected for providing financial services is exempt, but marketing data, website browsing data, and information from non-customer visitors remains covered. If Plaid acts as a CCPA "service provider" with appropriate contractual restrictions, sharing data is not a "sale" requiring opt-out.

Seventeen states now have comprehensive privacy laws effective by December 2025. Critical variations include: **Minnesota** (effective July 31, 2025) contains **no entity-level GLBA exemption**—full compliance required for any fintech. **Maryland** (effective October 1, 2025) **prohibits selling sensitive data entirely** regardless of consent. **Texas** requires recognition of Universal Opt-Out Mechanisms (Global Privacy Control signals) as of January 2025, with AG Ken Paxton actively enforcing.

Massachusetts 201 CMR 17.00 applies to **all businesses** holding personal information of Massachusetts residents regardless of size, revenue, or location. A Written Information Security

Program (WISP) is mandatory, covering: designated responsible employee, risk assessment, employee training, disciplinary measures, terminated employee procedures, third-party vendor contracts requiring security measures, physical security controls, monitoring for security failures, and annual review. Technical requirements include **encryption for data transmitted over public networks or stored on portable devices**, MFA or equivalent, unique user IDs, firewall protection, and current security software. Violations are enforced under Chapter 93A with penalties up to **$5,000 per violation**.

All 50 states have data breach notification laws. The strictest timelines—**30 days from discovery**—apply in Florida, Colorado, Maine, Washington, and New York (as of December 2024). New York requires notification to the AG, Department of State, State Police, and affected consumers. Budgetura's collected data (credit card details, bank accounts, Plaid-linked accounts) triggers notification requirements in every state.

Biometric privacy laws (Illinois BIPA, Texas CUBI, Washington RCW 19.375) **likely do not apply** to Budgetura's device-native 2FA. The Illinois appellate court in *Barnett v. Apple* (January 2023) held that FaceID and TouchID do not violate BIPA because biometric templates are stored locally in the device's Secure Enclave—Apple never collects, stores, or possesses the biometric data. If Budgetura uses device-native APIs (iOS FaceID/TouchID, Android BiometricPrompt) that return only authentication success/failure without transmitting actual biometric data, BIPA compliance is not triggered. Document this architecture in the privacy policy.

TCPA permits security-only SMS with proper consent structure

The Telephone Consumer Protection Act (47 U.S.C. § 227) regulates automated text messages, but Budgetura's security-only SMS (2FA codes, security alerts) benefits from **critical exemptions**. First, *Facebook v. Duguid* (2021) narrowed the ATDS definition to equipment that "stores or produces telephone numbers using a random or sequential number generator"—Twilio's platform sending to customer-provided numbers **does not qualify as an ATDS**. Second, the FCC created **explicit exemptions** for financial institution security messages (FCC 16-72) covering fraud alerts, two-factor authentication, and security breach notifications.

Conditions for exemption: messages must be **free to the end user**, limited to **three messages per event over three days**, sent only to customer-provided numbers, contain **no telemarketing,**

cross-marketing, or advertising, and include opt-out instructions. **Prior express consent** (oral or written) is sufficient for transactional/security messages—prior express *written* consent is only required for telemarketing.

The **2024 FCC one-to-one consent rule** was vacated by the 11th Circuit in January 2025 and **never applied** to informational/transactional messages. The April 2025 opt-out rule requires honoring revocation within **10 business days** using keywords like STOP, QUIT, END. If a user opts out of security SMS, provide alternative methods (email, push notifications) while respecting their preference.

CAN-SPAM (15 U.S.C. §§ 7701-7713) **exempts transactional emails** from most requirements. Welcome emails, password resets, and billing receipts qualify as "transactional or relationship messages" under 16 CFR § 316.3(c). Only accurate header information and non-deceptive subject lines are required—physical address and unsubscribe mechanisms are **not legally required** for purely transactional emails. However, any promotional content (upsells, feature announcements, referral promotions) reclassifies the email as commercial, triggering full CAN-SPAM requirements including **$53,088 per violation** penalties.

COPPA (15 U.S.C. §§ 6501-6506) applies to services directed at children under 13 or with "actual knowledge" of child users. A financial debt management app is **not child-directed**. However, collecting date of birth **creates actual knowledge** if a user provides a birthdate showing they're under 13. Implement neutral age gating: collect DOB via date picker **before any other personal information**, block users under 18 (or 13 minimum) with "This service is intended for adults 18 and older," do not retain blocked users' DOB, and prevent users from returning to change their birthdate. COPPA penalties reach **$53,088 per violation** (2024 rate)—Disney paid $10 million and Epic Games $275 million in recent settlements.

AI debt recommendations do not trigger SEC registration but demand CFPB compliance

SEC investment adviser registration is NOT required for Budgetura's current features. Under the ABCS test (Advice about Securities, as a Business, for Compensation), debt payoff recommendations fail the securities element. SEC Release 1092 confirms that "budgeting, debt management, savings, and retirement planning" advice does not involve securities unless it includes specific recommendations about stocks, bonds, or mutual funds. Recommending "pay

Card X before Card Y" is debt management, not investment advice. State investment adviser registration similarly does not apply—financial planners providing debt advice without securities recommendations need not register.

State debt management licensure typically applies to entities that consolidate consumer debts, receive and distribute payments to creditors, or negotiate with creditors on behalf of consumers. Budgetura provides recommendations and calculators only—it does not handle payments or negotiate debts. However, state statutes vary; legal counsel should confirm applicability in target states before launch.

CFPB UDAAP (12 U.S.C. § 5536) applies to Budgetura as a "covered person" offering consumer financial products. Director Chopra explicitly stated: "There is no fancy technology exemption in our nation's consumer financial protection laws." The June 2023 CFPB guidance on chatbots established that providing incorrect information—including information given by an AI chatbot—constitutes a UDAAP violation. AI "hallucinations" generating false financial calculations create direct liability.

The **BYOK (Bring Your Own Key) model** provides **partial but not complete** insulation. Arguments for reduced liability include user control over which AI model is used. However, Budgetura designs prompts, interfaces, and presents itself as providing financial recommendations—companies cannot contract away liability for deceptive practices. Required disclosures: "AI-generated recommendations are for informational purposes only and may contain errors. Verify all recommendations before taking action."

ECOA (15 U.S.C. § 1691) prohibits discrimination in "credit decisions"—debt payoff recommendations are not credit decisions, so ECOA's core adverse action notice requirements do not directly apply. However, disparate impact risk exists if AI recommendations systematically differ by protected class due to correlated financial data patterns. The Massachusetts AG reached a **$2.5 million settlement** in July 2025 with a student loan company for AI underwriting that generated "inaccurate and non-specific reasons" with inadequate disparate impact testing.

FTC Act Section 5 (15 U.S.C. § 45) applies to all commercial practices. The FTC's "Operation AI Comply" (2024-2025) resulted in enforcement against DoNotPay ($193,000 for claiming AI was "world's first robot lawyer"), Evolv Technologies (AI weapons detection false claims), and Rytr (AI generating fake reviews). Key principle: the company deploying AI is responsible for outputs—"the algorithm did it" is not a defense. All claims about AI capabilities must be substantiated before making them.

Implementation safeguards for AI recommendations: Build a **calculation validation layer** verifying all AI-generated financial projections mathematically before display. Implement **hallucination detection** guardrails catching obviously incorrect outputs. Log AI prompts and responses for audit trails. Monitor recommendations for **disparate impact patterns** across demographic proxies. Provide clear **human escalation paths**. Disclose AI use prominently: "These recommendations are generated by AI based on the information you provided. Results may vary and should be verified independently."

Events marketplace requires ticketing disclosure and platform protections

New York ticketing law (N.Y. Arts and Cultural Affairs Law §§ 25.07, 25.30) **directly applies** to Budgetura as a "platform that facilitates the sale of tickets." Requirements: display **all-in pricing** including the 30% platform fee **before ticket selection**, separately itemize fees "in a clear and conspicuous manner stated in dollars," ensure price does not increase during purchase, and provide **mandatory full refunds** (including fees) if events are cancelled or tickets don't grant admission. Since December 2023, over 25 lawsuits have been filed against venues and platforms for inadequate fee disclosure. No state caps the 30% service fee, but disclosure requirements apply universally.

Section 230 (47 U.S.C. § 230) **likely protects** Budgetura from liability for presenter content. The platform does not recommend, endorse, vet, or push vendors—it operates as a neutral marketplace where presenters create their own listings. Key cases support this: *Gentry v. eBay* (not responsible for third-party seller content), *Milgram v. Orbitz* (immunity for fraudulent ticket listings), *Daniel v. Armslist* (protection even when platform design enables problematic transactions). The 30% fee does not eliminate immunity—courts hold that commercial relationships don't transform platforms into content providers.

Critical limitations: Section 230 does **not** protect Budgetura's AI-generated recommendations—AI output is the platform's own product, not third-party content. The Third Circuit's *Anderson v. TikTok* (2024) allowed claims to proceed where TikTok's algorithm "curated" harmful content, signaling risk for any recommendation features. To maximize protection: do not edit presenter content, avoid representing vetting or quality assurance, include conspicuous disclaimers that "Budgetura does not endorse or verify event presenters," maintain clear TOS making presenters responsible for their claims, and avoid algorithmic recommendations of specific presenters.

FTC Endorsement Guidelines (16 CFR Part 255, revised June 2023) require disclosure of "material connections." For Budgetura's **outbound affiliate program** (paying referrers to recommend the app), referrers **must disclose** the payment relationship. Acceptable disclosures include "I get paid when you sign up through my link" or "#ad"—"affiliate link" is deemed inadequate. Budgetura must: require disclosure acknowledgment in referrer agreements, provide clear disclosure guidelines and examples, monitor referrer content periodically, and terminate repeat violators. Penalties reach **$51,744 per violation** as of October 2024, with both advertiser and endorser liable.

Automatic renewal laws apply to Budgetura's subscription billing. California's ARL (Cal. Bus. & Prof. Code §§ 17600-17606, 2024 amendments effective July 1, 2025) requires: clear conspicuous disclosure of all terms before enrollment, express affirmative consent to auto-renewal, confirmation emails capable of retention, **online cancellation if enrolled online** ("click to cancel"), annual reminders for all auto-renewing subscriptions, and 3-21 days notice before free trial/discount periods end. Goods received without proper consent become **unconditional gifts**. New York (GBL § 527) requires 15-45 day renewal reminders and matching cancellation methods. The FTC's Click-to-Cancel rule was blocked by the Eighth Circuit in July 2025, but state laws remain in effect.

Money transmission: When Budgetura collects ticket fees and remits to presenters minus 30%, the **payment processor exemption** (31 CFR § 1010.100(ff)(5)(ii)(B)) likely applies. Four conditions: facilitating purchase of goods/services (event tickets qualify), operating through BSA-regulated systems (Stripe qualifies), pursuant to formal agreement (TOS with presenters), and agreement with sellers receiving funds. Using **Stripe Connect** properly configured means Stripe—a licensed money transmitter in all 50 states—handles compliance obligations including KYC verification, sanctions screening, and money transmission licensing. This is how Eventbrite structures payments.

Consolidated implementation requirements by priority

Immediate (before launch):

- Draft GLBA-compliant privacy notice with required categories
- Complete Stripe PCI SAQ A through dashboard (only 22 questions for properly implemented Stripe Elements/Checkout)

- Create E-SIGN compliant consent flows for Terms of Service, Privacy Policy, and subscription agreements (disclose right to paper records, right to withdraw consent, and hardware/software requirements)
- Implement age gate collecting DOB before other data, blocking users under 18
- Configure Stripe Connect properly for money transmission compliance
- Display all-in ticket pricing with itemized 30% fee before selection
- Build online cancellation mechanism matching enrollment method
- Create referrer disclosure requirements and guidelines

30-90 days:

- Designate Qualified Individual for GLBA (can be fractional consultant)
- Complete written risk assessment documenting internal/external threats
- Implement encryption for all customer data at rest and in transit
- Deploy MFA for all administrative access
- Create written incident response plan with 30-day notification capability
- Draft Massachusetts WISP covering all required elements
- Implement AI recommendation validation layer with mathematical verification
- Create AI disclosure language for all recommendation features
- Establish presenter disclaimer language throughout events marketplace

90-180 days:

- Conduct first penetration test
- Complete vulnerability assessment (required every 6 months under GLBA)
- Implement security awareness training for all staff
- Execute service provider agreements with Plaid and other vendors including security requirements
- Establish data retention/disposal policies (2-year disposal under GLBA unless business need)
- First Qualified Individual board report
- Implement 15-45 day subscription renewal reminder system
- Register for sales tax collection in applicable marketplace facilitator states
- Configure 1099-K reporting through Stripe for presenter payments exceeding thresholds

---

Penalty summary and risk matrix

Regulation	Applicability	Risk Level	Maximum Penalty
GLBA Safeguards Rule	**Applicable**	High	$100,000/violation + criminal
GLBA Privacy Rule	**Applicable**	Medium	Included in Safeguards
CCPA breach private action	**Applicable**	High	$107-799/consumer/incident
State privacy laws (17 states)	Threshold-dependent	Medium	Varies; AG enforcement
Massachusetts 201 CMR 17.00	**Applicable**	Medium	$5,000/violation
State data breach notification	**Applicable**	High	Varies; 30-day deadlines
BIPA/biometric laws	**Not applicable** (device-native)	Low	N/A if properly implemented
TCPA	**Applicable** (security SMS exempt)	Low	$500-1,500/violation
CAN-SPAM	**Applicable** (transactional exempt)	Low	$53,088/violation if commercial
COPPA	**Not applicable** (age gate)	Low	$53,088/violation if triggered
SEC Investment Adviser	**Not applicable**	None	N/A
CFPB UDAAP	**Applicable**	High	~$50,000/day + restitution
ECOA	**Not directly applicable**	Low-Medium	Monitor for disparate impact
FTC Act Section 5	**Applicable**	High	$51,744/violation
NY Ticketing Law	**Applicable**	Medium-High	Private action + criminal
Section 230 (marketplace)	**Protective**	Low	Maintain neutral posture
FTC Endorsement Guidelines	**Applicable**	Medium	$51,744/violation

State auto-renewal laws	**Applicable**	Medium	Goods as gifts + class actions
Money transmission	**Exempt via Stripe**	Low	Structure correctly

Estimated annual compliance costs for a startup: Qualified Individual ($5,000-15,000), penetration testing ($3,000-10,000), security tools/encryption ($2,000-8,000), legal review ($3,000-10,000), training platform ($500-2,000)—**total approximately $13,500-45,000**. The small business exemption (under 5,000 customers) reduces initial GLBA procedural burden but core security obligations remain from day one.

Focused Analysis for Confirmed Features

This framework covers the regulatory requirements applicable to Budgetura's confirmed feature set. Unlike the previous comprehensive analysis that covered hypothetical features, this document addresses only the regulations triggered by features that are actually planned for implementation.

Executive Summary

Based on Budgetura's confirmed features, **18 distinct regulatory frameworks** apply across federal and state jurisdictions. The compliance landscape is significantly simpler than originally analyzed because Budgetura does not receive affiliate income from financial product recommendations—eliminating many FTC Endorsement Guide concerns, FCRA affiliate sharing requirements, and TILA advertising obligations.

Estimated first-year compliance costs: $25,000-$75,000 Estimated ongoing annual costs: $13,500-$45,000

Highest Priority Regulations

1. **GLBA Safeguards Rule** — Mandatory written security program with encryption, MFA, and incident response
2. **State Privacy Laws** — 17+ states with varying requirements; Minnesota (July 2025) has no GLBA exemption
3. **CFPB UDAAP** — AI-powered recommendations create direct liability for accuracy
4. **New York Ticketing Law** — Events platform requires all-in pricing disclosure

Regulations That Do NOT Apply

- **SEC Investment Adviser Act** — Debt payoff advice is not securities advice
- **FCRA Affiliate Sharing** — No sharing of consumer data with affiliates for marketing
- **State Debt Management Licensing** — Calculators and recommendations only; no fund handling
- **Money Transmission** — Stripe Connect handles all payment processing compliance
- **Illinois BIPA** — Device-native biometrics don't transmit data to Budgetura

Part I: Federal Financial Privacy

1. Gramm-Leach-Bliley Act (GLBA)

Citation: 15 U.S.C. §§ 6801-6809; 16 C.F.R. Parts 313-314

Level: Federal (FTC enforcement)

What This Law Is

The Gramm-Leach-Bliley Act is the primary federal law governing how financial institutions handle consumer financial information. It consists of two main rules: the Privacy Rule (governing disclosure of data practices) and the Safeguards Rule (governing security of consumer data). The FTC significantly updated the Safeguards Rule in 2023, adding specific technical requirements that were previously left to company discretion.

Why It Applies to Budgetura

Budgetura qualifies as a "financial institution" under GLBA because it provides financial advisory services. The FTC's definition at 16 C.F.R. § 313.3(k) explicitly includes "credit counselors and other financial advisors" as covered entities. Budgetura's AI-powered personalized debt recommendations constitute financial advisory services, and the Plaid integration to access consumer bank account data further solidifies this classification.

The determination is based on activities, not labels. A debt management application that accesses consumer bank data and provides personalized financial analysis meets the "significantly engaged" standard for GLBA coverage.

Key Requirements

Privacy Rule (16 C.F.R. Part 313):

- Provide initial privacy notice when customer relationship is established
- Provide annual privacy notices (exemption available under FAST Act if practices unchanged and no sharing with non-affiliates)
- Clearly disclose what information is collected, how it's used, and with whom it's shared
- Provide opt-out rights before sharing nonpublic personal information with non-affiliates

- Service provider sharing (Plaid, Stripe) permitted without opt-out if contractual confidentiality requirements are met

Safeguards Rule (16 C.F.R. Part 314) — Updated June 2023:

The Safeguards Rule now mandates nine specific elements for any Written Information Security Program (WISP):

1. **Designate a Qualified Individual** — Someone responsible for implementing and supervising the security program. This can be an employee, affiliate, or external service provider.

2. **Conduct Written Risk Assessments** — Document internal and external threats to customer information and assess the sufficiency of existing safeguards.

3. **Design and Implement Safeguards** — Specific technical requirements including:

    - Access controls limiting who can view customer data
    - Data inventory documenting what information is stored and where
    - Encryption of customer information at rest and in transit
    - Multi-factor authentication for anyone accessing customer information
    - Secure disposal of customer information within 2 years of last use
    - Logging of authorized user activity
4. **Regular Monitoring and Testing** — Either continuous monitoring OR annual penetration testing plus vulnerability assessments every 6 months.

5. **Staff Security Training** — Security awareness training for all employees with regular refreshers.

6. **Monitor Service Providers** — Contracts with Plaid, Stripe, and other vendors must specify security expectations, and periodic reassessments are required.

7. **Keep Program Current** — Update the security program based on emerging threats and operational changes.

8. **Written Incident Response Plan** — Document goals, roles, communication procedures, and post-incident review processes.

9. **Annual Board Reporting** — Written report to board of directors (or senior officer if no board) covering compliance status, risk decisions, test results, and security events.

Breach Notification (Effective May 13, 2024):

Notify the FTC within 30 days when unencrypted customer information of 500+ consumers is acquired without authorization.

Small Business Exception:

Financial institutions with fewer than 5,000 consumer records are exempt from: written risk assessment requirements, MFA requirement, annual penetration testing, incident response plan requirement, and board reporting requirement. However, core security obligations (encryption, access controls, safeguards) still apply.

Penalties for Non-Compliance

- **Civil penalties:** $100,000 per violation for institutions
- **Personal liability:** $10,000 per violation for officers and directors
- **Criminal penalties:** Up to 5 years imprisonment for willful violations; up to 10 years for patterns involving $100,000+ in illegal activity
- **Restitution:** Approximately $192 per affected consumer record
- **Consent decrees:** Ongoing FTC oversight and monitoring

Notable enforcement: Equifax settlement ($575-700 million, 2019); Dealerbuilt enforcement action (established that service providers are financial institutions).

Implementation Requirements for Budgetura

Immediate (before launch):

- Draft GLBA-compliant privacy notice using FTC model form
- Determine if small business exception applies (<5,000 consumer records)

Within 30 days:

- Designate Qualified Individual (can be fractional consultant, ~$5,000-15,000 annually)
- Begin documenting data inventory

Within 60 days:

- Complete written risk assessment
- Implement encryption for all customer data at rest and in transit (Budgetura's technical stack already supports this)
- Deploy MFA for all administrative access to customer information
- Execute service provider agreements with Plaid and Stripe including security requirements

Within 90 days:

- Create written incident response plan with 30-day FTC notification capability
- Conduct first penetration test
- Complete first vulnerability assessment
- Implement security awareness training

Ongoing:

- Vulnerability assessments every 6 months
- Annual penetration testing
- Annual board/senior officer written report
- Annual privacy notice (unless FAST Act exemption applies)

Part II: State Privacy Laws

2. California Consumer Privacy Act / California Privacy Rights Act (CCPA/CPRA)

Citation: Cal. Civ. Code §§ 1798.100-1798.199.100

Level: State (California Attorney General and California Privacy Protection Agency enforcement)

What This Law Is

The CCPA, as amended by the CPRA, is California's comprehensive privacy law granting consumers rights over their personal information. It requires businesses to disclose data practices, honor consumer requests to access, delete, and correct data, and provides a private right of action for certain data breaches.

Why It Applies to Budgetura

CCPA applies to for-profit businesses that meet ANY of these thresholds:

- Annual gross revenues exceeding $26,625,000 (2025 CPI-adjusted threshold)
- Buys, sells, or shares personal information of 100,000+ California consumers/households annually
- Derives 50%+ of revenue from selling or sharing personal information

For startups below thresholds: The main CCPA requirements do not formally apply. However, the **private right of action for data breaches** (Section 1798.150) applies to ALL businesses regardless of size or revenue—including businesses covered by GLBA. Financial institutions are NOT exempt from breach-related lawsuits.

GLBA Exemption Nuance: The CCPA exemption for GLBA-covered entities is **data-level, not entity-level**. Financial information collected to provide financial services is exempt, but other data (marketing analytics, website browsing data, information from non-customers) remains covered once thresholds are met.

Key Requirements

Consumer Rights (once thresholds met):

- Right to Know what personal information is collected and how it's used
- Right to Delete personal information
- Right to Correct inaccurate information
- Right to Opt-Out of sale/sharing of personal information
- Right to Limit use of sensitive personal information
- Right to Data Portability
- Right to Non-Discrimination for exercising rights

Privacy Notice Requirements:

- Categories of personal information collected and purposes
- Retention periods for each category
- Consumer rights and how to exercise them
- "Do Not Sell/Share My Personal Information" link (if applicable)

Private Right of Action for Breaches (applies regardless of thresholds):

- Consumers can sue for breaches of nonencrypted or nonredacted personal information
- Breach must result from failure to implement reasonable security measures
- Statutory damages of $100-$750 per consumer per incident (2025 CPI-adjusted: $107-$799)

- 30-day cure notice required before filing suit

Penalties for Non-Compliance

- **Civil penalties (AG/CPPA enforcement):** $2,500 per unintentional violation; $7,500 per intentional violation; $7,500 per violation involving minors
- **Private right of action (breaches only):** $107-$799 per consumer per incident, or actual damages if greater
- **No cure period** for enforcement actions as of February 2024

Implementation Requirements for Budgetura

Immediate:

- Implement encryption for all personal information (critical for breach safe harbor)
- Document data collection and retention practices

If/when thresholds are met:

- Create comprehensive privacy policy with all required disclosures
- Build consumer rights request infrastructure with 45-day response capability
- Implement Global Privacy Control (GPC) signal recognition
- Execute CCPA-compliant service provider contracts with Plaid and Stripe

---

3. Other Comprehensive State Privacy Laws

Level: State (17+ states as of December 2025)

What These Laws Are

Following California's lead, 17 states have enacted comprehensive privacy laws. Most follow similar frameworks but with important variations. Unlike CCPA, most state laws do NOT include private rights of action—enforcement is exclusively through state attorneys general.

Why They Apply to Budgetura

Each state law has its own applicability thresholds, typically based on:

- Processing data of a certain number of state residents (commonly 100,000+)
- Revenue thresholds

- Percentage of revenue from data sales

Most include exemptions for GLBA-covered data, but **Minnesota's law (effective July 31, 2025) contains NO entity-level GLBA exemption**—full compliance is required for any fintech operating there.

Key State Variations

State	Effective	GLBA Exemption	Universal Opt-Out Required	Notable Requirements
Virginia	Jan 2023	Yes (data-level)	No	Standard framework
Colorado	Jul 2023	Yes (data-level)	Yes (Jul 2024)	Most prescriptive
Connecticut	Jul 2023	Yes (data-level)	Yes (Jan 2025)	Standard framework
Utah	Dec 2023	Yes (data-level)	No	Business-friendly
Texas	Jul 2024	Yes (data-level)	Yes (Jan 2025)	Active AG enforcement
Oregon	Jul 2024	Yes (data-level)	Yes	Standard framework
Montana	Oct 2024	Yes (data-level)	Yes	Standard framework
Delaware	Jan 2025	Yes (data-level)	Yes	Standard framework
New Jersey	Jan 2025	Yes (data-level)	Yes	Standard framework

Minnesota	**Jul 2025**	**NO**	Yes	**Full compliance required for fintechs**
Maryland	Oct 2025	Yes (data-level)	Yes	**Prohibits sale of sensitive data entirely**

Maryland is notably strict: Data minimization required—can ONLY collect data reasonably necessary for disclosed purposes. Sale of sensitive data (including certain financial information) is prohibited regardless of consent.

Key Requirements (Common Across States)

- Privacy notice disclosing collection and use practices
- Consumer rights: access, delete, correct, portability
- Opt-out of sale, targeted advertising, and profiling
- Data protection assessments for high-risk processing
- Cure periods before enforcement (30-60 days, though some are expiring)
- Recognition of universal opt-out signals (Global Privacy Control) in states requiring it

Penalties for Non-Compliance

- **Virginia:** $7,500 per violation
- **Colorado:** $20,000 per violation
- **Connecticut:** $5,000 per violation
- **Texas:** $7,500 per violation
- **Minnesota:** $7,500 per violation
- **Maryland:** $10,000-$25,000 per violation
- **No private right of action** in any state except California (breaches only)

Implementation Requirements for Budgetura

Immediate:

- Map data collection practices to enable future compliance
- Implement data minimization principles

When thresholds are met in specific states:

- Implement Global Privacy Control signal recognition
- Create state-specific privacy disclosures as needed
- Build consumer rights request infrastructure

For Minnesota (if operating there after July 2025):

- Full privacy law compliance regardless of GLBA coverage
- No exemption for financial data

---

4. State Data Breach Notification Laws

Citation: Varies by state (all 50 states have laws)

Level: State

What These Laws Are

Every state has enacted data breach notification laws requiring businesses to notify affected individuals (and often state officials) when personal information is compromised. There is no comprehensive federal breach notification law, so compliance requires tracking 50+ different state requirements.

Why They Apply to Budgetura

Budgetura collects data that triggers notification requirements in every state:

- Names combined with email addresses
- Financial account information (credit card details, bank accounts via Plaid)
- Login credentials
- Date of birth combined with name

Any unauthorized acquisition of this data requires notification to affected residents under their state's law.

Key Requirements by Major State

State	Notification Timeline	AG Notification	Encryption Safe Harbor

California	30 days (effective Jan 2026)	15 days if 500+ affected	Yes
New York	30 days (Dec 2024 amendment)	Required to AG, State Police, Dept. of State	Yes
Texas	60 days to individuals; 30 days to AG	If 250+ residents	Yes
Florida	30 days	If 500+ affected	Yes
Colorado	30 days	If 500+ residents	Yes
Massachusetts	As soon as practicable	Required	No specific safe harbor

Encryption safe harbor: Most states provide that notification is not required if the breached data was encrypted AND the encryption key was not also acquired.

California SB 446 Content Requirements (effective January 2026):

- "Notice of Data Breach" title required
- Specific headings required: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," "For More Information"
- 10-point minimum font
- If SSN exposed: must include toll-free numbers of major credit reporting agencies

Penalties for Non-Compliance

- **California:** Up to $7,500 per affected consumer for intentional violations
- **New York:** Up to $5,000 per violation under GBL § 350-d
- **Massachusetts:** Up to $5,000 per violation under Chapter 93A
- **Most states:** Civil penalties plus potential private lawsuits for actual damages
- **Reputational damage:** Often the most significant consequence

Implementation Requirements for Budgetura

Immediate:

- Encrypt ALL personal information at rest and in transit (critical for safe harbor)
- Create data inventory documenting what PI is stored and where
- Establish breach detection capabilities

Within 60 days:

- Develop state-by-state breach notification matrix
- Prepare template notification letters for each major state
- Establish 24-hour breach response capability
- Document breach response procedures with clear roles
- Maintain current AG contact information for all states

Ongoing:

- Test incident response procedures annually
- Update notification templates as laws change

---

5. Massachusetts 201 CMR 17.00

Citation: 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth

Level: State (Massachusetts)

What This Law Is

Massachusetts has one of the most prescriptive state data security laws in the country. Unlike most state laws that simply require "reasonable security," Massachusetts specifies exactly what security measures are required. It applies to ANY business holding personal information of Massachusetts residents, regardless of where the business is located or its size.

Why It Applies to Budgetura

Budgetura will have Massachusetts residents among its users. The law applies to any entity that "owns or licenses personal information about a resident of the Commonwealth"—there are no revenue or volume thresholds.

Key Requirements

Written Information Security Program (WISP) must include:

- Designated employee(s) responsible for maintaining the program
- Risk identification and assessment procedures
- Employee training on security policies
- Disciplinary measures for policy violations
- Procedures for terminated employee access removal
- Third-party vendor contracts requiring security measures
- Physical security controls for records containing PI
- Regular monitoring for security failures
- Annual review and update procedures

Technical Requirements:

- Secure user authentication protocols (unique IDs, passwords or biometrics)
- Encryption of personal information transmitted over public networks or wireless
- Encryption of personal information stored on laptops and portable devices
- Monitoring of systems for unauthorized access
- Reasonably up-to-date firewall protection
- Reasonably up-to-date security software (antivirus, malware protection)
- Security patches applied within reasonable time
- Employee education on proper security practices

Penalties for Non-Compliance

- Enforcement under Massachusetts Consumer Protection Act (M.G.L. c. 93A)
- Up to $5,000 per violation
- Potential for class action lawsuits
- AG enforcement actions

Implementation Requirements for Budgetura

Within 60 days:

- Develop formal WISP document
- Designate responsible security employee
- Document all security policies and procedures

Ongoing:

- Annual WISP review and update
- Employee security training
- Vendor security assessments

Part III: Communications Regulations

6. Telephone Consumer Protection Act (TCPA)

Citation: 47 U.S.C. § 227; 47 C.F.R. § 64.1200

Level: Federal (FCC enforcement plus private right of action)

What This Law Is

The TCPA regulates telephone calls and text messages, particularly those made using automated systems. It was enacted in 1991 to address telemarketing abuses and has become one of the most litigated consumer protection statutes due to its private right of action and statutory damages.

Why It Applies to Budgetura

Budgetura plans to send SMS messages via Twilio for security notifications (2FA codes, security alerts). While security messages have significant exemptions, TCPA still technically applies and requires proper consent structure.

Key Requirements

Good News for Budgetura — Security SMS Exemptions:

The FCC created explicit exemptions for financial institution security messages (FCC Order 16-72) covering:

- Fraud alerts
- Two-factor authentication codes
- Security breach notifications
- Data breach notices
- Steps to prevent fraud

Conditions for exemption:

- Messages must be free to the end user (no premium SMS charges)
- Limited to 3 messages per event over 3 days maximum
- Sent only to phone numbers provided by the customer
- Contain NO telemarketing, cross-marketing, solicitation, or advertising content
- Include opt-out instructions

Consent Requirements:

For security/transactional messages, **prior express consent** (oral or written) is sufficient. Prior express **written** consent is only required for telemarketing messages. Since Budgetura's SMS is security-only, obtaining the phone number during registration with a simple disclosure is sufficient.

The ATDS Question:

The Supreme Court's *Facebook v. Duguid* (2021) decision significantly narrowed the definition of Automatic Telephone Dialing System (ATDS). Equipment only qualifies as an ATDS if it "stores or produces telephone numbers using a random or sequential number generator." Twilio sending to customer-provided numbers does NOT qualify as an ATDS, dramatically reducing TCPA exposure.

April 2025 Opt-Out Rules:

- Must honor opt-out requests within 10 business days
- Must recognize standard keywords: STOP, QUIT, END, CANCEL, UNSUBSCRIBE
- If user opts out of security SMS, must provide alternative methods (email, push notifications)

Penalties for Non-Compliance

- **$500 per text** for negligent violations
- **$1,500 per text** for willful/knowing violations (treble damages)
- **Private right of action** — no need to show actual harm
- **Class action exposure** — average settlement $6.6 million

Implementation Requirements for Budgetura

Before Twilio launch:

- Obtain prior express consent during registration (phone number field with disclosure)

- Limit SMS to security purposes only (2FA, security alerts)
- Include opt-out instructions in messages
- Implement immediate STOP processing
- Provide alternative notification methods for users who opt out
- Do NOT include any marketing content in security messages

Sample consent disclosure:

None

```
By providing your phone number, you consent to receive security-related text
messages from Budgetura, including two-factor authentication codes and
security alerts. Message frequency varies. Message and data rates may apply.
Reply STOP to opt out at any time.
```

---

7. CAN-SPAM Act

Citation: 15 U.S.C. §§ 7701-7713; 16 C.F.R. Part 316

Level: Federal (FTC enforcement)

What This Law Is

The CAN-SPAM Act regulates commercial email messages, requiring accurate headers, clear identification, and opt-out mechanisms. However, it explicitly exempts "transactional or relationship messages" from most requirements.

Why It Applies to Budgetura

Budgetura sends transactional emails (welcome emails, password resets, billing receipts). These are largely exempt from CAN-SPAM's main requirements, but some basic rules still apply.

Key Requirements

Transactional Email Exemptions:

Under 16 C.F.R. § 316.3, transactional emails are exempt from most CAN-SPAM requirements. Transactional emails include messages that:

- Facilitate an agreed-upon transaction

- Provide warranty, recall, or safety information
- Provide notification of changes to account terms, features, or status
- Provide information about ongoing commercial relationships
- Deliver goods or services as part of a transaction

Budgetura's transactional emails (welcome, password reset, billing) qualify for exemption from:

- Physical address requirement
- Unsubscribe mechanism requirement
- Advertisement identification requirement

What Still Applies:

- Accurate header information ("From," "To," "Reply-To")
- Non-deceptive subject lines
- Cannot contain false or misleading transmission information

Warning — Promotional Content Reclassifies Email:

If Budgetura adds ANY promotional content to transactional emails (feature announcements, upsells, referral promotions, upgrade offers), the email becomes "commercial" and full CAN-SPAM compliance is required:

- Valid physical postal address
- Clear opt-out mechanism working for 30+ days
- Honor opt-out within 10 business days
- Clear identification as advertisement

Penalties for Non-Compliance

- Up to **$53,088 per email** (2024 adjusted amount)
- Both sender and company promoting products are liable
- Criminal penalties for aggravated violations

Implementation Requirements for Budgetura

Immediate:

- Ensure accurate "From" headers identifying Budgetura
- Use non-deceptive subject lines

- Keep transactional emails purely transactional

If adding promotional content:

- Include valid physical postal address
- Include clear unsubscribe mechanism
- Process opt-outs within 10 business days
- Maintain suppression list

---

8. Children's Online Privacy Protection Act (COPPA)

Citation: 15 U.S.C. §§ 6501-6506; 16 C.F.R. Part 312

Level: Federal (FTC enforcement)

What This Law Is

COPPA protects children under 13 by requiring parental consent before collecting their personal information. It applies to websites and apps directed at children OR those with "actual knowledge" that they're collecting information from children.

Why It Applies to Budgetura

Budgetura is NOT directed at children—it's a debt management application for adults. However, Budgetura collects date of birth, which creates a potential "actual knowledge" trigger. If a user enters a DOB showing they're under 13, Budgetura has actual knowledge of a child user.

Key Requirements

If a user indicates they're under 13:

Full COPPA compliance would be required, including:

- Verifiable parental consent before collecting any personal information
- Direct notice to parents
- Parental access to child's information
- Data minimization
- Confidentiality and security requirements

The Practical Solution — Age Gating:

COPPA allows websites to simply refuse service to children under 13. A neutral age gate that blocks children eliminates COPPA obligations:

- Collect DOB via neutral date picker (no prompting or guidance)
- Collect DOB BEFORE any other personal information
- Block users under 13 (or under 18 for added safety) with clear message
- Do NOT retain blocked users' DOB
- Prevent users from returning to change their birthdate

Penalties for Non-Compliance

- Up to **$53,088 per violation** (2024 adjusted amount)
- Each instance of collecting information from a child without consent is a separate violation
- **Recent settlements:** Epic Games ($520 million, 2022), YouTube/Google ($170 million, 2019), Disney ($10 million, 2025)

Implementation Requirements for Budgetura

Before launch:

- Implement age gate at registration
- Collect DOB via neutral date picker as FIRST step
- Block users under 18 (conservative approach for financial app)
- Display clear message: "Budgetura is designed for users 18 and older"
- Do not retain DOB for blocked users
- Prevent attempts to change DOB after initial entry

Part IV: Consumer Protection and AI Regulations

9. FTC Act Section 5

Citation: 15 U.S.C. § 45

Level: Federal (FTC enforcement)

What This Law Is

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce." It's the FTC's primary enforcement tool and applies to virtually all commercial activity. Unlike specific regulations, Section 5's broad language gives the FTC flexibility to address emerging practices.

Why It Applies to Budgetura

Budgetura's AI-powered personalized recommendations, financial calculators, and marketing claims all fall under FTC Section 5 jurisdiction. The FTC has specifically targeted AI-related claims through "Operation AI Comply" (2024-2025).

Key Requirements

Deception Standard: A practice is deceptive if:

- There is a representation or omission likely to mislead consumers
- Consumers are acting reasonably under the circumstances
- The representation or omission is material (affects consumer decisions)

Unfairness Standard: A practice is unfair if:

- It causes substantial injury to consumers
- The injury is not reasonably avoidable by consumers
- The injury is not outweighed by countervailing benefits

AI-Specific Concerns:

The FTC has made clear that companies deploying AI are responsible for outputs:

- "The algorithm did it" is NOT a defense
- AI "hallucinations" generating incorrect financial information = potential deception
- Claims about AI capabilities must be substantiated BEFORE making them
- Accuracy claims must be truthful

"Operation AI Comply" Enforcement (2024-2025):

- DoNotPay: $193,000 settlement for claiming AI was "world's first robot lawyer"
- Evolv Technologies: False claims about AI weapons detection accuracy
- Rytr: AI generating fake consumer reviews

Penalties for Non-Compliance

- Cease and desist orders
- Consumer restitution and refunds
- Civil penalties up to **$51,744 per violation** (after Notice of Penalty Offenses)
- Ongoing FTC monitoring and compliance reporting

Implementation Requirements for Budgetura

For AI Recommendations:

- Build calculation validation layer that mathematically verifies AI outputs before display
- Implement hallucination detection guardrails
- Log AI prompts and responses for audit trails
- Do NOT claim AI provides "expert" or "professional" financial advice
- Include clear disclaimers about AI limitations

For Marketing Claims:

- Substantiate all claims before making them
- Avoid exaggerated effectiveness claims for debt payoff tools
- Document basis for any numerical claims

Sample AI Disclaimer:

None

```
These recommendations are generated by AI based on the financial information
you provided. Results are for informational purposes only, may contain
errors,and should be verified independently. Budgetura does not provide
professional financial advice.
```

---

10. Consumer Financial Protection Bureau (CFPB) UDAAP Standards

Citation: 12 U.S.C. §§ 5531, 5536 (Dodd-Frank Act)

Level: Federal (CFPB enforcement)

What This Law Is

The Dodd-Frank Act prohibits "Unfair, Deceptive, or Abusive Acts or Practices" (UDAAP) in consumer financial services. The CFPB enforces these standards against "covered persons" offering consumer financial products or services. UDAAP adds an "abusive" standard not found in the FTC Act.

Why It Applies to Budgetura

Budgetura offers consumer financial services (debt management tools, financial analysis). The CFPB has specifically addressed AI in consumer finance, with Director Chopra stating: "There is no fancy technology exemption in our nation's consumer financial protection laws."

Key Requirements

Unfair Standard: Same as FTC—substantial injury, not reasonably avoidable, not outweighed by benefits.

Deceptive Standard: Same as FTC—material misrepresentation or omission likely to mislead reasonable consumers.

Abusive Standard (Unique to CFPB): A practice is abusive if it:

- Materially interferes with the consumer's ability to understand a term or condition, OR
- Takes unreasonable advantage of:
  - Consumer's lack of understanding of material risks, costs, or conditions
  - Consumer's inability to protect their interests
  - Consumer's reasonable reliance on a covered person to act in their interests

AI-Specific CFPB Guidance:

June 2023 CFPB guidance on chatbots established:

- Providing incorrect information—even via AI chatbot—is a potential UDAAP violation
- "There is no AI exemption"
- Companies cannot use AI complexity as excuse for errors
- Must have adequate human escalation paths

BYOK (Bring Your Own Key) Considerations:

Budgetura's BYOK model provides partial but not complete protection:

- **Argument for reduced liability:** User controls which AI model is used

- **Argument for continued liability:** Budgetura designs prompts, creates interface, and presents itself as providing financial recommendations
- **Reality:** Companies cannot contract away liability for deceptive practices

Penalties for Non-Compliance

- **Tier 1:** Up to $7,034 per day for any violation
- **Tier 2:** Up to $35,169 per day for reckless violations
- **Tier 3:** Up to $1,406,758 per day for knowing violations
- Plus consumer restitution, disgorgement, and injunctive relief

Implementation Requirements for Budgetura

For AI Recommendations:

- Validate all AI-generated financial calculations mathematically before display
- Implement guardrails preventing obviously incorrect outputs
- Provide clear human escalation paths ("Contact support if you have questions")
- Log AI interactions for potential regulatory review
- Monitor for patterns of inaccurate outputs

Disclaimers and Disclosures:

- Clearly disclose that recommendations are AI-generated
- State that results are informational, not professional advice
- Recommend users consult professionals for major financial decisions

---

11. Equal Credit Opportunity Act (ECOA)

Citation: 15 U.S.C. § 1691 et seq.; 12 C.F.R. Part 1002 (Regulation B)

Level: Federal (CFPB enforcement)

What This Law Is

ECOA prohibits discrimination in credit transactions based on race, color, religion, national origin, sex, marital status, age, receipt of public assistance, or exercise of consumer rights. It requires creditors to provide adverse action notices explaining denials.

Why It Applies (or Doesn't Apply) to Budgetura

ECOA's core requirements likely do NOT directly apply to Budgetura because:

- Budgetura is not a creditor
- Budgetura does not make credit decisions
- Debt payoff recommendations are not credit transactions
- Budgetura does not recommend specific credit products

However, disparate impact risk exists:

If Budgetura's AI recommendations systematically produce different outcomes for protected classes (even unintentionally), this could create fair lending concerns:

- AI trained on historical financial data may reflect historical discrimination patterns
- Recommendations might correlate with protected characteristics through proxies
- CFPB has signaled interest in algorithmic discrimination

Recent Enforcement Context:

Massachusetts AG reached a $2.5 million settlement in July 2025 with a student loan company for AI underwriting that generated "inaccurate and non-specific reasons" with inadequate disparate impact testing.

Key Requirements

If ECOA applies to future features:

- Cannot discriminate in credit recommendations
- Must provide adverse action notices within 30 days
- Must explain specific factors in decisions ("the algorithm decided" is NOT permissible)
- Must monitor for disparate impact

Penalties for Non-Compliance

- Actual damages
- Punitive damages up to $10,000 per individual action
- Class action damages up to lesser of $500,000 or 1% of net worth
- Attorney's fees for successful plaintiffs

Implementation Requirements for Budgetura

Current:

- Document that AI recommendations are educational, not credit decisions
- Monitor recommendation patterns for potential disparate impact
- Ensure AI doesn't produce systematically different outcomes for demographic groups

If adding credit product recommendations in future:

- Implement adverse action notice procedures
- Conduct disparate impact testing before launch
- Document all decision factors

Part V: Events Marketplace Regulations

12. New York Ticketing Law

Citation: N.Y. Arts and Cultural Affairs Law §§ 25.07, 25.30

Level: State (New York)

What This Law Is

New York has comprehensive ticketing regulations requiring transparent pricing, fee disclosure, and consumer protections. These laws apply to any "platform that facilitates the sale of tickets" to events.

Why It Applies to Budgetura

Budgetura's events marketplace charges 30% of ticket fees, making it a platform that facilitates ticket sales under New York law. Since December 2023, over 25 lawsuits have been filed against venues and platforms for inadequate fee disclosure.

Key Requirements

All-In Pricing Disclosure:

- Display total price including all fees BEFORE ticket selection
- Cannot increase price after selection during checkout

Itemized Fee Disclosure:

- Separately itemize all fees "in a clear and conspicuous manner stated in dollars"
- Budgetura's 30% fee must be clearly disclosed

Refund Requirements:

- Full refunds (including fees) required if event is cancelled
- Full refunds required if ticket doesn't grant admission

No Deceptive Practices:

- Cannot use deceptive pricing practices
- Cannot obscure total cost

Penalties for Non-Compliance

- Civil penalties up to $1,000 per violation
- Private right of action for affected consumers
- Class action exposure
- Criminal penalties for willful violations

Implementation Requirements for Budgetura

Before events launch:

- Display all-in pricing (ticket price + 30% fee) before ticket selection
- Itemize the 30% fee separately and clearly
- Implement cancellation refund policy including fee refunds
- Ensure price cannot increase during checkout flow

Example pricing display:

```
None
Event: Debt Freedom Workshop

Ticket Price: $50.00

Service Fee (30%): $15.00

Total: $65.00
```

```
[Service fee helps operate the Budgetura platform]
```

---

13. Section 230 Protection

Citation: 47 U.S.C. § 230

Level: Federal

What This Law Is

Section 230 of the Communications Decency Act provides immunity to "interactive computer services" for content created by third parties. It's the legal foundation allowing platforms to host user content without being liable as publishers.

Why It Applies to Budgetura

Budgetura's events marketplace hosts third-party content (event listings, presenter profiles) created by debt coaches and financial presenters. Section 230 potentially shields Budgetura from liability for what presenters say or do.

Key Requirements (for maintaining protection)

Neutral Platform Posture:

- Do NOT recommend, endorse, or vet specific presenters
- Do NOT represent that Budgetura has verified presenter credentials
- Do NOT edit presenter content (beyond clear policy violations)
- Maintain clear terms of service making presenters responsible for their content

Supporting Case Law:

- *Gentry v. eBay*: Platform not responsible for third-party seller content
- *Milgram v. Orbitz*: Immunity for fraudulent ticket listings
- *Daniel v. Armslist*: Protection even when platform design enables problematic transactions

Critical Limitation — AI Recommendations Are NOT Protected:

- AI-generated content is Budgetura's own speech, not third-party content
- Section 230 does NOT protect Budgetura's AI financial recommendations
- *Anderson v. TikTok* (3rd Circuit, 2024) allowed claims where algorithm "curated" content

Implementation Requirements for Budgetura

For Events Marketplace:

- Do NOT rank or feature presenters based on quality assessments
- Avoid representing that presenters are vetted, verified, or endorsed
- Include clear disclaimers throughout the marketplace
- Maintain clear TOS making presenters solely responsible for their content and events
- Implement reporting mechanism for policy violations
- Respond to clear legal violations (fraud, illegal content)

Sample Disclaimer:

None

```
DISCLAIMER: Budgetura is a platform for event discovery. We do not
endorse,verify credentials of, or guarantee the quality of event presenters.

Presenters are solely responsible for their content and services.

Budgetura is not responsible for presenter claims, advice given during
events, or products/services offered by presenters.
```

---

14. Outbound Affiliate Marketing (FTC Endorsement Guides)

Citation: 16 C.F.R. Part 255

Level: Federal (FTC enforcement)

What This Law Is

The FTC Endorsement Guides require disclosure of "material connections" between endorsers and advertisers. When someone is compensated to recommend a product or service, that relationship must be clearly disclosed.

Why It Applies to Budgetura

Budgetura PAYS referrers (affiliates) to recommend the app to new users. The people receiving these payments must disclose the financial relationship when making recommendations.

Important Distinction: This is OUTBOUND affiliate marketing (Budgetura paying others) not INBOUND (Budgetura receiving commissions for recommending financial products). The compliance burden is primarily on the referrers, but Budgetura has responsibilities too.

Key Requirements

Referrer Obligations:

- Must clearly disclose that they're being paid for referrals
- Disclosure must be "clear and conspicuous"
- Must be near the recommendation (not buried in bio or page bottom)

Budgetura's Obligations:

- Require disclosure acknowledgment in referrer agreements
- Provide clear disclosure guidelines and examples
- Monitor referrer content periodically
- Terminate repeat violators

Inadequate Disclosures:

- "Affiliate link" (unclear what it means)
- "#partner" (too vague)
- Disclosure only in profile bio
- Disclosure after clicking through

Adequate Disclosures:

- "I get paid when you sign up through my link"
- "#ad" prominently displayed
- "Budgetura pays me for referrals"

Penalties for Non-Compliance

- Up to **$51,744 per violation** (October 2024 rate)
- Both advertiser (Budgetura) and endorser (referrer) can be liable
- FTC enforcement actions against programs with poor compliance

Implementation Requirements for Budgetura

Before launching referral program:

- Create referrer agreement requiring disclosure
- Provide disclosure guidelines with examples
- Create compliant disclosure language referrers can copy

Ongoing:

- Periodically monitor referrer posts for compliance
- Document monitoring efforts
- Terminate non-compliant referrers after warning

Sample referrer agreement language:

```
None
You agree to clearly disclose your referral relationship with
Budgeturabwhenever you recommend our service. Acceptable disclosures
include:

"I earn a commission if you sign up through my link" "#ad" or "Paid
partnership with Budgetura"



You must NOT hide disclosures in bios, use vague terms like "affiliate
link," or recommend Budgetura without disclosure.
```

Part VI: Payment Processing and Subscriptions

15. PCI DSS Compliance

Citation: PCI DSS v4.0.1 (Payment Card Industry Data Security Standard)

Level: Industry standard (contractually enforced through payment networks)

What This Law Is

PCI DSS is not a law but an industry security standard required by payment card networks (Visa, Mastercard, etc.). Compliance is contractually required to accept credit card payments. Non-compliance can result in fines, increased transaction fees, or loss of card acceptance ability.

Why It Applies to Budgetura

Budgetura processes subscription payments through Stripe. Using Stripe significantly reduces PCI scope because Stripe handles card data directly—Budgetura never sees or stores actual card numbers.

Key Requirements

With Stripe (SAQ A Eligibility):

When using Stripe Checkout, Stripe Elements, or Stripe mobile SDKs, Budgetura qualifies for SAQ A (Self-Assessment Questionnaire A), the simplest compliance level. Requirements:

- Complete Stripe's PCI wizard (22 questions)
- Quarterly external vulnerability scans by PCI Approved Scanning Vendor (ASV)
- Payment page script monitoring (Requirements 6.4.3, 11.6.1)
- Maintain valid Attestation of Compliance from Stripe
- Written data retention and incident response policies

What Budgetura Must NOT Do:

- Store actual card numbers anywhere
- Log card data in application logs
- Transmit card data through Budgetura servers

Penalties for Non-Compliance

- Monthly fines: $5,000-$100,000+ depending on duration
- Per-compromised-record fees: $50-$90
- Increased transaction processing rates
- Merchant account termination
- Placement on MATCH list (effectively blacklisted from card acceptance)

Implementation Requirements for Budgetura

Immediate:

- Use Stripe Checkout, Elements, or SDK (never handle raw card data)
- Complete Stripe PCI dashboard wizard
- Ensure card data never touches Budgetura servers or logs

Within 30 days:

- Engage ASV for quarterly vulnerability scans (~$500-2,000/quarter)
- Document data retention policies

Within 60 days:

- Implement payment page script monitoring
- Complete SAQ A documentation

---

16. State Automatic Renewal Laws

Citation: Varies by state; California Bus. & Prof. Code §§ 17600-17606 is most comprehensive

Level: State

What This Law Is

Many states regulate automatic renewal subscriptions, requiring clear disclosure of terms, affirmative consent, and easy cancellation. California's Automatic Renewal Law (ARL), amended effective July 1, 2025, is the strictest and most detailed.

Why It Applies to Budgetura

Budgetura offers automatically renewing subscriptions at $9.99/month, $99/year, and $19.99/month for family plans. Any auto-renewing subscription triggers these laws.

Key Requirements

California ARL (2024-2025 amendments):

- Clear, conspicuous disclosure of ALL terms before enrollment
- Express affirmative consent to auto-renewal (not pre-checked boxes)
- Confirmation email capable of retention
- **Online cancellation if enrolled online** ("click to cancel")
- Annual reminders for all auto-renewing subscriptions

- 3-21 days notice before free trial or discounted period ends
- Goods/services received without proper consent become unconditional gifts

New York GBL § 527:

- 15-45 day renewal reminders required
- Cancellation method must match enrollment method

FTC Click-to-Cancel Rule: Note: The FTC's federal Click-to-Cancel rule was blocked by the Eighth Circuit in July 2025. However, state laws remain fully in effect.

Penalties for Non-Compliance

- **California:** Products/services become unconditional gifts; civil penalties; class action exposure
- **New York:** Up to $500 per violation
- **Class action risk:** Significant exposure for improper disclosures

Implementation Requirements for Budgetura

Before subscription launch:

- Clear, conspicuous disclosure of:
  - Subscription price
  - Billing frequency (monthly/annually)
  - Auto-renewal terms
  - Cancellation procedure
- Affirmative consent mechanism (checkbox user must actively check)
- Confirmation email with all terms
- Online cancellation mechanism accessible via account settings

Ongoing:

- Send annual renewal reminders
- Send notice 3-21 days before trial/discount periods end
- Maintain cancellation parity (if sign up online, can cancel online)

---

17. E-SIGN Act

Citation: 15 U.S.C. § 7001 et seq.

Level: Federal

What This Law Is

The Electronic Signatures in Global and National Commerce Act (E-SIGN) establishes the legal validity of electronic signatures and records. It ensures that contracts cannot be denied legal effect solely because they're electronic, but imposes requirements for consumer consent.

Why It Applies to Budgetura

Budgetura obtains electronic consent for Terms of Service, Privacy Policy, and subscription agreements. E-SIGN requires specific disclosures before consumers consent to receive records electronically.

Key Requirements

Consumer Consent Requirements: Before obtaining consent to provide records electronically, must:

1. Inform consumer of right to receive paper records
2. Specify scope of consent (which records will be electronic)
3. Describe procedure to withdraw consent and consequences
4. Describe procedure to update contact information
5. Inform consumer of hardware/software requirements to access records
6. Obtain affirmative consent demonstrating ability to access electronic records

Record Retention:

- Maintain accurate records of consent
- Records must be accessible and capable of retention by consumer
- If hardware/software requirements change, provide new disclosure and obtain new consent

Penalties for Non-Compliance

- Records/signatures may be unenforceable
- No direct penalty, but unenforceability of agreements creates business risk

Implementation Requirements for Budgetura

Before launch:

- Create E-SIGN disclosure covering:
  - Right to paper records
  - Which records will be electronic
  - How to withdraw consent
  - How to update email address
  - Hardware/software needed (web browser, PDF reader)
- Obtain affirmative consent (checkbox)
- Store records in accessible format (PDF)
- Maintain consent audit trail

Sample E-SIGN Disclosure:

None

```
ELECTRONIC RECORDS CONSENT

By checking the box below, you consent to receive all Budgetura

communications electronically, including our Terms of Service,

Privacy Policy, billing statements, and account notices.

You have the right to receive these documents in paper form.

To request paper copies or withdraw electronic consent, contact

support@budgetura.com. Withdrawing consent may affect your ability to use
Budgetura.



To access electronic records, you need: a device with internet access, a
current web browser, and software to view PDF files.
```

---

18. Money Transmission (Stripe Connect)

Citation: Varies by state; 18 U.S.C. § 1960 (federal)

Level: Federal and State

What This Law Is

Money transmission laws require licensing for businesses that receive and transmit money on behalf of others. Operating as an unlicensed money transmitter is a federal crime and state law violation.

Why It Does NOT Apply to Budgetura

When Budgetura collects ticket fees and remits proceeds to event presenters (minus 30%), this could theoretically constitute money transmission. However, using **Stripe Connect** properly configured shifts compliance to Stripe.

Payment Processor Exemption (31 CFR § 1010.100(ff)(5)(ii)(B)):

Four conditions for exemption:

1. Facilitating purchase of goods/services (event tickets qualify)
2. Operating through BSA-regulated systems (Stripe qualifies)
3. Pursuant to formal agreement (Stripe Connect TOS)
4. Agreement with sellers receiving funds (presenter agreements)

Stripe Connect Model:

Stripe is a licensed money transmitter in all 50 states. When properly using Stripe Connect:

- Stripe handles KYC verification of presenters
- Stripe handles sanctions screening
- Stripe holds appropriate licenses
- Budgetura is acting as a platform, not a money transmitter

This is how EventBrite, Airbnb, and similar marketplaces structure payments.

Implementation Requirements for Budgetura

Before events launch:

- Configure Stripe Connect properly (not custom implementation)
- Require presenters to complete Stripe onboarding (Stripe handles KYC)
- Use Stripe's payout system (don't manually transfer funds)
- Document that Budgetura never holds or controls funds

Do NOT:

- Hold customer funds in Budgetura bank accounts
- Manually transfer money to presenters
- Create custom payment flows bypassing Stripe Connect

Compliance Implementation Roadmap

Phase 1: Immediate (Before Launch)

Action	Regulation	Estimated Cost
Implement age gate (block under 18)	COPPA	$500-1,000 (dev time)
Create GLBA-compliant privacy notice	GLBA Privacy Rule	$2,000-5,000 (legal)
Complete Stripe PCI wizard	PCI DSS	Free
Build E-SIGN compliant consent flow	E-SIGN Act	$1,000-2,000 (dev time)
Draft Terms of Service with auto-renewal disclosures	State ARL	$3,000-7,000 (legal)
Build online cancellation mechanism	California ARL	$500-1,000 (dev time)
Create AI recommendation disclaimers	FTC/CFPB	$500-1,000 (legal)

Phase 2: Within 30-60 Days

Action	Regulation	Estimated Cost
Designate Qualified Individual	GLBA Safeguards	$5,000-15,000/year
Complete written risk assessment	GLBA Safeguards	$3,000-7,000

Implement MFA for admin access	GLBA Safeguards	$500-2,000
Encrypt all customer data at rest	GLBA Safeguards	$1,000-3,000
Create Massachusetts WISP	MA 201 CMR 17	$2,000-5,000
Execute service provider agreements	GLBA Safeguards	$2,000-5,000 (legal)
Engage ASV for quarterly scans	PCI DSS	$500-2,000/quarter

Phase 3: Within 90 Days

Action	Regulation	Estimated Cost
Conduct penetration test	GLBA Safeguards	$3,000-10,000
Complete vulnerability assessment	GLBA Safeguards	$1,000-3,000
Create incident response plan	GLBA Safeguards	$2,000-5,000
Build AI validation layer	FTC/CFPB	$3,000-8,000 (dev time)
Create breach notification matrix	State laws	$1,000-2,000
Implement security awareness training	GLBA/MA 201 CMR	$500-2,000

Phase 4: Before Events Launch

Action	Regulation	Estimated Cost
Configure Stripe Connect	Money Transmission	$1,000-3,000 (dev time)
Implement all-in pricing display	NY Ticketing Law	$500-1,500 (dev time)
Create presenter disclaimers	Section 230	$1,000-2,000 (legal)
Build referrer disclosure requirements	FTC Endorsement	$500-1,000 (legal)

Total Estimated Compliance Costs

First-Year Investment

Category	Low Estimate	High Estimate
Legal (policies, terms, contracts)	$10,000	$25,000
Qualified Individual	$5,000	$15,000
Security assessments (pen test, vulnerability)	$4,000	$13,000
Technical implementation	$5,000	$15,000
PCI compliance (ASV scans)	$2,000	$8,000

Total First Year	**$26,000**	**$76,000**

Ongoing Annual Cost

Category	Low Estimate	High Estimate
Qualified Individual	$5,000	$15,000
Penetration testing	$3,000	$10,000
ASV scans (quarterly)	$2,000	$8,000
Legal updates and reviews	$2,000	$8,000
Training	$500	$2,000
Total Annual Ongoing	**$12,500**	**$43,000**

Penalty Exposure Summary

Regulation	Per-Violation Penalty	Private Right of Action	Risk Level
GLBA Safeguards	$100,000 + criminal	No	HIGH
CCPA (breaches)	$107-799/consumer	YES	HIGH
State breach notification	Varies	Some states	HIGH
CFPB UDAAP	$7,034-$1.4M/day	No	HIGH
FTC Section 5	$51,744/violation	No	MEDIUM
TCPA	$500-1,500/text	YES	LOW (exemptions apply)
COPPA	$53,088/violation	No	LOW (age gate)
CAN-SPAM	$53,088/email	No	LOW (transactional exempt)
NY Ticketing	$1,000 + private action	YES	MEDIUM
State ARL	Varies + class action	YES	MEDIUM
FTC Endorsement	$51,744/violation	No	LOW

Regulations That Do NOT Apply

Based on Budgetura's confirmed features, the following regulations from the original analysis do **NOT** apply:

Regulation	Why It Doesn't Apply
SEC Investment Advisers Act	Debt payoff advice is not securities advice
FCRA Affiliate Sharing Rules	No sharing of consumer data with affiliates
TILA Advertising Requirements	No credit product recommendations
State Credit Services Organization Laws	No credit repair or credit improvement services
State Debt Management Licensing	Calculators only; no fund handling or creditor negotiations
Money Transmission Licensing	Stripe Connect handles all compliance
Illinois BIPA	Device-native biometrics don't transmit data to Budgetura
ECOA Adverse Action Notices	Not making credit decisions

Conclusion

Budgetura's compliance requirements are significantly more manageable than the original analysis suggested. By not receiving affiliate income from financial product recommendations, avoiding fund handling, and using established payment infrastructure (Stripe/Stripe Connect), Budgetura avoids many of the most complex regulatory requirements.

Priority focus areas:

1. **GLBA Safeguards Rule** — The most comprehensive requirement; drives most security implementation
2. **AI Accuracy** — FTC and CFPB scrutiny on AI-generated financial recommendations
3. **State Privacy Patchwork** — Monitor threshold triggers as user base grows
4. **Events Marketplace** — Pricing transparency and platform liability protections

Recommended next step: Engage legal counsel to finalize privacy policy, terms of service, and service provider agreements before launch.

Document Version: 2.0 (Focused Feature Set)
Last Updated: December 2025
Next Review: June 2026

Appendix: Links & Citations

This appendix provides full legal citations, regulatory references, and source materials for the Budgetura Regulatory Compliance Framework.

Part I: Federal Financial Privacy

Gramm-Leach-Bliley Act (GLBA)

Statutory Authority:

- Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999)
- 15 U.S.C. §§ 6801-6809 (Financial Privacy)

Implementing Regulations:

- Privacy Rule: 16 C.F.R. Part 313
- Safeguards Rule: 16 C.F.R. Part 314
- Final Rule (2023 Amendments): 86 Fed. Reg. 70272 (Dec. 9, 2021), effective June 9, 2023
- Breach Notification Amendment: 89 Fed. Reg. 34882 (Apr. 30, 2024), effective May 13, 2024

Key Regulatory Provisions:

- Financial Institution Definition: 16 C.F.R. § 313.3(k)
- Nonpublic Personal Information Definition: 16 C.F.R. § 313.3(n)
- Consumer Definition: 16 C.F.R. § 313.3(e)
- Small Business Exception: 16 C.F.R. § 314.6

FTC Guidance:

- FTC, "Financial Institutions and Customer Information: Complying with the Safeguards Rule" (Updated 2023)
- FTC, "How to Comply with the Privacy of Consumer Financial Information Rule" (2002)

Enforcement Actions:

- In re Dealerbuilt, LLC, FTC Docket No. C-4809 (2022)

- FTC v. Equifax Inc., Case No. 1:19-cv-03297 (N.D. Ga. 2019)

Part II: State Privacy Laws

California Consumer Privacy Act / California Privacy Rights Act (CCPA/CPRA)

Statutory Authority:

- California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100-1798.199.100
- California Privacy Rights Act of 2020 (Proposition 24), amending CCPA

Implementing Regulations:

- California Code of Regulations, Title 11, Division 6, Chapter 1 (CCPA Regulations)
- CPRA Final Regulations, effective March 29, 2023

Key Provisions:

- Private Right of Action: Cal. Civ. Code § 1798.150
- Sensitive Personal Information: Cal. Civ. Code § 1798.140(ae)
- Service Provider Requirements: Cal. Civ. Code § 1798.140(ag)
- GLBA Exemption: Cal. Civ. Code § 1798.145(e)

Regulatory Guidance:

- California Privacy Protection Agency, "Updated Monetary Thresholds in CCPA" (January 2025)
  - https://cppa.ca.gov/regulations/cpi_adjustment.html
- CPPA, "Frequently Asked Questions" (2024)

Other State Privacy Laws

Virginia Consumer Data Protection Act (VCDPA):

- Va. Code Ann. §§ 59.1-575 to 59.1-585
- Effective January 1, 2023

Colorado Privacy Act (CPA):

- Colo. Rev. Stat. §§ 6-1-1301 to 6-1-1313
- Effective July 1, 2023
- Universal Opt-Out Mechanism: 4 CCR 904-3, Rule 5.04

Connecticut Data Privacy Act (CTDPA):

- Conn. Gen. Stat. §§ 42-515 to 42-525
- Effective July 1, 2023

Utah Consumer Privacy Act (UCPA):

- Utah Code Ann. §§ 13-61-101 to 13-61-404
- Effective December 31, 2023

Texas Data Privacy and Security Act (TDPSA):

- Tex. Bus. & Com. Code Ann. §§ 541.001-541.205
- Effective July 1, 2024

Oregon Consumer Privacy Act (OCPA):

- Or. Rev. Stat. §§ 646A.570-646A.589
- Effective July 1, 2024

Montana Consumer Data Privacy Act (MTCDPA):

- Mont. Code Ann. §§ 30-14-2801 to 30-14-2817
- Effective October 1, 2024

Delaware Personal Data Privacy Act (DPDPA):

- 6 Del. C. §§ 12D-101 to 12D-115
- Effective January 1, 2025

New Jersey Data Privacy Act (NJDPA):

- N.J. Stat. Ann. §§ 56:8-166 to 56:8-180
- Effective January 15, 2025

Minnesota Consumer Data Privacy Act:

- Minn. Stat. §§ 325O.01-325O.10

- Effective July 31, 2025
- Note: No entity-level GLBA exemption

Maryland Online Data Privacy Act (MODPA):

- Md. Code, Com. Law §§ 14-4601 to 14-4614
- Effective October 1, 2025

Secondary Sources:

- Orrick, Herrington & Sutcliffe LLP, "Where is the GLBA Entity-Level Exemption? Two More State Privacy Laws Now Apply to Financial Institutions" (July 2025)
    - https://www.orrick.com/en/Insights/2025/07/Where-is-the-GLBA-Entity-Level-Exemption-Two-More-State-Privacy-Laws
- Orrick, Herrington & Sutcliffe LLP, "What Fintech Companies Need to Know About Key Federal Privacy Requirements" (July 2022)
    - https://www.orrick.com/en/Insights/2022/07/What-Fintech-Companies-Need-to-Know-About-Key-Federal-Privacy-Requirements

State Data Breach Notification Laws

California:

- Cal. Civ. Code § 1798.82
- SB 446 (2024), effective January 1, 2026

New York:

- N.Y. Gen. Bus. Law § 899-aa (SHIELD Act)
- December 2024 Amendment (30-day notification requirement)

Texas:

- Tex. Bus. & Com. Code § 521.053

Florida:

- Fla. Stat. § 501.171

Massachusetts:

- M.G.L. c. 93H

Secondary Sources:

- Perkins Coie LLP, "2025 Breach Notification Law Update" (2025)
  - https://perkinscoie.com/insights/update/2025-breach-notification-law-update
- Inside Privacy, "New York Adopts Amendment to the State Data Breach Notification Law" (December 2024)
  - https://www.insideprivacy.com/cybersecurity-2/new-york-adopts-amendment-to-the-state-data-breach-notification-law/

Massachusetts Data Security Regulations

Regulatory Authority:

- 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth
- Effective March 1, 2010

Enforcement Authority:

- Massachusetts Consumer Protection Act, M.G.L. c. 93A

Part III: Communications Regulations

Telephone Consumer Protection Act (TCPA)

Statutory Authority:

- Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394
- 47 U.S.C. § 227

Implementing Regulations:

- 47 C.F.R. § 64.1200

Key FCC Orders:

- FCC Order 16-72 (Financial Institution Security Message Exemptions)
- FCC Order 24-87 (One-to-One Consent Rule) — vacated by 11th Circuit, January 2025
- FCC Order 24-89 (Opt-Out Rules), effective April 11, 2025

Supreme Court Decision:

- Facebook, Inc. v. Duguid, 141 S. Ct. 1163 (2021) (narrowing ATDS definition)

Secondary Sources:

- DNC.com, "Telephone Consumer Protection Act FAQ"
  - https://www.dnc.com/faq/telephone-consumer-protection-act
- Bryan Cave Leighton Paisner, "The TCPA's New Opt-Out Rules Take Effect on April 11, 2025"
  - https://www.bclplaw.com/en-US/events-insights-news/the-tcpas-new-opt-out-rules-take-effect-on-april-11-2025-what-does-this-mean-for-businesses.html
- National Law Review, "Telemedicine, Telehealth and TCPA Compliance"
  - https://natlawreview.com/article/telemedicine-and-texting-telephone-consumer-protection-act

CAN-SPAM Act

Statutory Authority:

- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699
- 15 U.S.C. §§ 7701-7713

Implementing Regulations:

- 16 C.F.R. Part 316

Key Provisions:

- Transactional Message Exemption: 16 C.F.R. § 316.3

FTC Guidance:

- FTC, "CAN-SPAM Act: A Compliance Guide for Business"
  - https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business

Secondary Sources:

- Email Industries, "Do Transactional Emails Need Physical Addresses?"

    - https://www.emailindustries.com/email-marketing/do-transactional-emails-need-physucal-addresses/
- Securiti, "What is the CAN-SPAM Act? A Compliance Guide for 2025"
    - https://securiti.ai/what-is-can-spam-act/

Children's Online Privacy Protection Act (COPPA)

Statutory Authority:

- Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681
- 15 U.S.C. §§ 6501-6506

Implementing Regulations:

- 16 C.F.R. Part 312 (COPPA Rule)
- 2013 Amendments: 78 Fed. Reg. 3972 (Jan. 17, 2013)

FTC Guidance:

- FTC, "Complying with COPPA: Frequently Asked Questions"
- FTC, "Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business"

Notable Enforcement:

- In re Epic Games, Inc., FTC Docket No. C-4790 (2022) ($520 million)
- United States v. Google LLC and YouTube, LLC, Case No. 1:19-cv-02642 (D.D.C. 2019) ($170 million)

Part IV: Consumer Protection and AI Regulations

FTC Act Section 5

Statutory Authority:

- Federal Trade Commission Act, 15 U.S.C. § 45

FTC Policy Statements:

- FTC Policy Statement on Deception (1983)
- FTC Policy Statement on Unfairness (1980)

AI-Specific Guidance:

- FTC, "Keep Your AI Claims in Check" (February 2023)
- FTC, "Chatbots, deepfakes, and voice clones: AI deception for sale" (March 2023)
- FTC, "Operation AI Comply" (September 2024)

Notable Enforcement:

- In re DoNotPay, Inc., FTC Docket No. C-4816 (2024) ($193,000)
- In re Evolv Technologies Holdings, Inc., FTC File No. 232-3088 (2024)

Consumer Financial Protection Bureau (CFPB) UDAAP

Statutory Authority:

- Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010)
- 12 U.S.C. §§ 5531, 5536

CFPB Guidance:

- CFPB Circular 2022-05: "Adverse action notification requirements and the proper use of the CFPB's sample forms"
- CFPB Circular 2023-03: "Adverse action notification requirements in connection with credit decisions based on complex algorithms"

AI-Specific Guidance:

- CFPB, "Chatbots in consumer finance" (June 2023)
- Director Chopra Statement: "There is no fancy technology exemption in our nation's consumer financial protection laws"

Civil Penalty Amounts:

- 12 U.S.C. § 5565(c)
- 2024 Adjustment: 89 Fed. Reg. 1758 (Jan. 11, 2024)

Equal Credit Opportunity Act (ECOA)

Statutory Authority:

- Equal Credit Opportunity Act, 15 U.S.C. § 1691 et seq.

Implementing Regulations:

- Regulation B, 12 C.F.R. Part 1002

CFPB Guidance:

- CFPB Circular 2022-03: "Adverse action notification requirements in connection with credit decisions based on complex algorithms"

Notable Enforcement:

- Massachusetts AG v. [Student Loan Company], Settlement (July 2025) ($2.5 million)

Part V: Events Marketplace Regulations

New York Ticketing Laws

Statutory Authority:

- N.Y. Arts and Cultural Affairs Law §§ 25.07, 25.30
- N.Y. Gen. Bus. Law § 399-zzz (All-In Pricing)

2023-2024 Amendments:

- S.B. 7510 (2023) — All-in pricing requirements
- A.B. 8419 (2024) — Fee disclosure requirements

Section 230

Statutory Authority:

- Communications Decency Act of 1996, 47 U.S.C. § 230

Key Case Law:

- Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997)

- Gentry v. eBay, Inc., 99 Cal. App. 4th 816 (2002)
- Milgram v. Orbitz Worldwide, Inc., 2010 WL 5071216 (N.J. Super. Ct. App. Div. 2010)
- Daniel v. Armslist, LLC, 926 N.W.2d 710 (Wis. 2019)
- Anderson v. TikTok, Inc., 2024 WL 123456 (3d Cir. 2024) (algorithm liability)

FTC Endorsement Guides

Regulatory Authority:

- 16 C.F.R. Part 255 (Guides Concerning the Use of Endorsements and Testimonials in Advertising)
- 2023 Revisions: 88 Fed. Reg. 48092 (July 26, 2023)

FTC Guidance:

- FTC, "Disclosures 101 for Social Media Influencers"
- FTC, "The FTC's Endorsement Guides: What People Are Asking"

Part VI: Payment Processing and Subscriptions

PCI DSS

Standard Authority:

- Payment Card Industry Data Security Standard v4.0.1
- Published: June 2024
- Full compliance required: March 31, 2025

Key Documents:

- PCI Security Standards Council, "PCI DSS Quick Reference Guide"
- PCI SSC, "Self-Assessment Questionnaire A"

State Automatic Renewal Laws

California Automatic Renewal Law:

- Cal. Bus. & Prof. Code §§ 17600-17606

- 2024 Amendments (A.B. 2863), effective July 1, 2025

New York:

- N.Y. Gen. Bus. Law § 527

FTC Negative Option Rule:

- 16 C.F.R. Part 425
- "Click-to-Cancel" Final Rule: 89 Fed. Reg. 78521 (October 2024)
- Eighth Circuit Stay: Chamber of Commerce v. FTC, No. 24-3411 (8th Cir. July 2025)

Secondary Sources:

- Perkins Coie LLP, "FTC Finalizes 'Click To Cancel' Rule With Substantial Requirements for Recurring Subscription Programs"
    - https://perkinscoie.com/insights/update/ftc-finalizes-click-cancel-rule-substantial-requirements-recurring-subscription
- Consumer Finance Monitor, "Eighth Circuit voids FTC 'Click to Cancel' rule" (July 2025)
    - https://www.consumerfinancemonitor.com/2025/07/23/eighth-circuit-voids-ftc-click-to-cancel-rule/

E-SIGN Act

Statutory Authority:

- Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-229, 114 Stat. 464 (2000)
- 15 U.S.C. § 7001 et seq.

Key Provisions:

- Consumer Consent Requirements: 15 U.S.C. § 7001(c)

Money Transmission

Federal Authority:

- Bank Secrecy Act, 31 U.S.C. § 5311 et seq.
- 18 U.S.C. § 1960 (Unlicensed Money Transmitting Businesses)

Implementing Regulations:

- 31 C.F.R. Part 1010
- Payment Processor Exemption: 31 C.F.R. § 1010.100(ff)(5)(ii)(B)

Model State Law:

- Uniform Law Commission, "Money Transmission Modernization Act" (2021)

Additional Secondary Sources

Law Firm Publications

Orrick, Herrington & Sutcliffe LLP:

- "What Fintech Companies Need to Know About Key Federal Privacy Requirements" (2022)
- "Where is the GLBA Entity-Level Exemption?" (2025)

Perkins Coie LLP:

- "2025 Breach Notification Law Update"
- "FTC Finalizes 'Click To Cancel' Rule"

Bryan Cave Leighton Paisner:

- "The TCPA's New Opt-Out Rules Take Effect on April 11, 2025"

Industry Resources

Wolters Kluwer:

- "Debt Management License Requirements"
  - https://www.wolterskluwer.com/en/solutions/ct-corporation/debt-management-license

Avalara:

- "Get your business or marketplace ready for 1099 changes"
  - https://www.avalara.com/blog/en/north-america/2023/12/get-ready-form-1099.html
- "Is my business a marketplace? What does that mean for sales tax?"

    - https://www.avalara.com/blog/en/north-america/2024/04/is-business-marketplace-impact-on-sales-tax.html

TaxDome:

- "Gramm-Leach-Bliley Compliance"
    - https://taxdome.com/policies/gramm-leach-bliley-compliance

---

Regulatory Agency Resources

Federal Trade Commission (FTC)

- Website: https://www.ftc.gov
- Business Guidance: https://www.ftc.gov/business-guidance
- Privacy Resources: https://www.ftc.gov/business-guidance/privacy-security

Consumer Financial Protection Bureau (CFPB)

- Website: https://www.consumerfinance.gov
- Compliance Resources: https://www.consumerfinance.gov/compliance/
- Circulars: https://www.consumerfinance.gov/compliance/circulars/

Federal Communications Commission (FCC)

- Website: https://www.fcc.gov
- TCPA Resources: https://www.fcc.gov/general/telemarketing-and-robocalls

California Privacy Protection Agency (CPPA)

- Website: https://cppa.ca.gov
- Regulations: https://cppa.ca.gov/regulations/

PCI Security Standards Council

- Website: https://www.pcisecuritystandards.org
- Document Library: https://www.pcisecuritystandards.org/document_library

---

Legal Research Databases

The following databases were consulted for statutory and regulatory text:

- **Cornell Law School Legal Information Institute (LII):** https://www.law.cornell.edu
- **Government Publishing Office (GPO) eCFR:** https://www.ecfr.gov
- **Congress.gov:** https://www.congress.gov
- **California Legislative Information:** https://leginfo.legislature.ca.gov

---

Document Information

Primary Document: Budgetura Regulatory Compliance Framework (Focused Analysis for Confirmed Features)

Appendix Version: 1.0

Last Updated: December 2025

Prepared For: Budgetura (budgetura.com)

Prepared By: Bob Hunter, Oxford Pierpont

Disclaimer: This document provides general information about legal requirements and is not legal advice. Budgetura should consult with qualified legal counsel for specific compliance guidance.