WILSON ELSER

Safira A. Castro

Associate

safira.castro@wilsonelser.com
Denver, CO – 303.385.4855

Safira Castro represents clients in actual or suspected cybersecurity incidents and data breaches, from business email compromises to ransomware attacks and data exfiltration events. She is a member of Wilson Elser's 24/7 incident response team, advising private and public companies across all industry sectors.

Safira regularly counsels clients on their legal obligations under U.S. and international data privacy and breach notification laws and assists in devising remediation strategies. She also helps organizations transform regulatory complexity into practical, resilient governance frameworks, designing enterprise-wide programs that map and manage personal, sensitive, and high-risk data flows in compliance with the expanding landscape of domestic and international privacy and AI laws. She brings more than seven years of experience spanning law firm, Big Four consulting, and in-house environments.

Before joining Wilson Elser, Safira defended clients in class action and complex cybersecurity matters for a regional civil defense litigation firm and served as a cyber regulatory legal consultant at IBM, advising the chief information security officer and internal business units on risk-based compliance with emerging regulations. She began her career as a senior associate at PricewaterhouseCoopers, where she advised Fortune 500 clients on privacy program development, regulatory compliance, and data protection impact assessments.

Incident Response
Safira guides clients through the full lifecycle of data security incidents, from initial investigation and containment through regulatory notification and post-incident remediation. She coordinates with forensic experts, insurers, and co-counsel to develop tailored response strategies and assists clients in navigating crisis communications during active incidents.

Data Privacy & Regulatory Compliance
Safira counsels regulated entities, government contractors, and global enterprises on compliance with a broad spectrum of domestic and international privacy regulations, including the GDPR, CCPA/CPRA, GLBA, DORA, NIS2, BIPA, and CIPA.

Services

- Cybersecurity & Data Privacy

Cybersecurity & Privacy Litigation
Safira has experience defending clients in class action litigation and complex cybersecurity disputes across federal and state courts. Her litigation experience includes pixel claims, CIPA demands, data breach class actions, and matters arising from ransomware and data exfiltration events. She has aided in resolving data breach litigation through motions to dismiss and has handled pre-litigation matters, including settling CIPA demands prior to suit.

Technology Transactions & Contracts
Safira drafts and negotiates data protection agreements, SaaS contracts, service agreements, and other technology-related commercial contracts. She has advised clients across diverse sectors, including software/technology, telecommunications, healthcare, fintech, pharmaceuticals, and federal contracting. She brings additional experience in emerging risk areas such as infrastructure law, IoT, post-quantum encryption, and cryptographic resilience.

Education

- Northeastern University School of Law (J.D., 2019)
- University of Florida (B.A. Political Science)
    - International Relations Certificate
    - Minor in Italian Language Studies

Bar Admissions

- Colorado

Court Admissions

- U.S. District Court, District of Colorado

Professional Affiliations

- International Association of Privacy Professionals (IAPP)
- Colorado Bar Association

Languages

- Spanish
- Italian

Representative Matters

Aided in obtaining successful dismissals and favorable settlements in data breach litigation matters through effective motions practice.

Resolved pre-litigation CIPA demands on behalf of clients prior to the filing of formal

complaints.

Advised Fortune 500 businesses on compliance strategies to mitigate civil and criminal liability risks arising from multiple cybersecurity frameworks, including NIST frameworks, Executive Order 14028, and the False Claims Act.