NELSON MULLINS

FinTech University

FinTech and Data Privacy
March 7, 2023

Risks of Failure to Comply

- In October 2020, the OCC assessed a $60 million civil money penalty against Morgan Stanley
- Morgan Stanley failed to exercise proper oversight of the 2016 decommissioning of two Wealth Management business data centers located in the United States
- Amongst other things, the banks failed to:
    - Effectively assess or address risks associated with decommissioning its hardware,
    - Adequately assess the risk of subcontracting the decommissioning work, including exercising adequate due diligence in selecting a vendor and monitoring its performance, and
    - Maintain appropriate inventory of customer data stored on the decommissioned hardware devices.

What is the Gramm-Leach-Bliley Act?

Two Rules	
Privacy Notice Rule	**Safeguards Rule**
Applies to businesses that are "significantly engaged" in “financial activities.”	Ensures financial institutions implement safeguards to identify and control privacy risks.

Privacy Notice Rule

The Privacy Notice Rule only applies to institutions that are "significantly engaged" in **"financial activities"**

- Whether the Rule applies to your business or not depends on the conduct of your business
- "**Financial activities**"* include:
  - Lending, exchanging, transferring, investing for others, or safeguarding money or securities
  - Providing financial, investment or economic advisory services. Brokering and servicing loans
  - Debt collecting
  - Providing real estate settlement services
  - Career counseling (of individuals seeking employment in the financial services industry)
- Which businesses might these activities cover?
  - Traditional Banks, Lenders, Wire Transfer Services, Sellers of Money Orders, Credit Counselors, Financial Planners, Tax Preparers, Accountants, and Investment Advisors, amongst others

* Under Section 4(k) of the Bank Holding Company Act and Federal Reserve Board regulations

Privacy Notice Rule: Do you have customers or consumers?

- Privacy Notice Rule obligations depend on whether your clients are “customers” or “consumers”

Client type	How is this client type defined?	Do I need to give this client type notice of my privacy practices?	Examples
 **Consumers**	Consumers are those who obtain a financial product or service from a financial institution primarily for personal, family, or household purposes.	Only required to give notice of privacy practices to consumers if you use their information in certain ways.	• Making a wire transfer • Cashing a check with a check-cashing company
 **Customers**	Customers are a sub-class of consumers who have a continuing relationship with a financial institution. Customers are defined by the nature of the relationship with the financial institution, not the duration.	Must give notice of privacy policy to ALL customers.	• Opening a credit card account • Leasing a car from an auto-dealer

- Considerations for “light users” of FinTechs

Safeguards 2.0

Updated Definition of "Financial Institution"

New Requirements for Safeguarding Data

Safeguards 2.0 - New Definition of “Financial Institution”

- traditional banking functions;
- making, brokering, or servicing extensions of credit;
- property appraising;
- collection services;
- credit reporting;
- asset management;
- leasing property;
- real estate settlement; and
- bringing together buyers and sellers of any product or service that the parties negotiate and consummate

Safeguards 2.0 – New Requirements

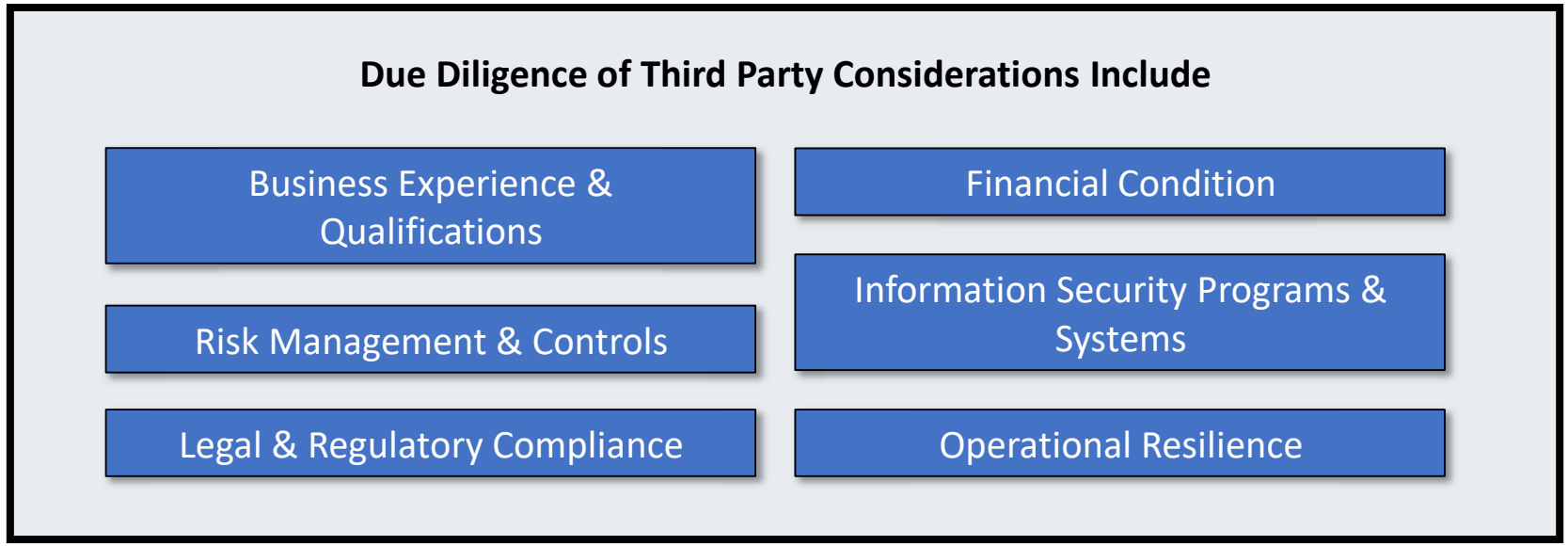
- *Qualified Individual Appointment*: All businesses must identify a qualified individual who can oversee and implement the information security program
- *Criteria for Risk Assessments:* Updated specific requirements for risk assessments
- *Additional Criteria for Implementing Safeguards:* Additional requirements for implementing safeguards for risks identified as part of the risk assessments
- *Information Security Monitoring and Penetration Testing*: Requires either continuous monitoring or periodic penetration testing
- *Training of Security Personnel*
- *Periodic Assessments of Service Providers*
- *Written Incident Response Plans*
- *Periodic Reports to the Board of Directors*

Focus on Resolving Identified Risks

- The Revised Safeguards Rule focuses on ensuring that financial institutions are implementing safeguards to control the risks identified through the risk assessment including:
  - Implementing and periodically reviewing access controls
  - Knowing what the financial institution has in its information ecosystem and where it is located
  - Encrypting customer information within the system and when in transit
  - Assessing any applications that store, access, or transmit customer information
  - Implementing multi-factor authentication for anyone accessing customer information on your system
  - Disposing of customer information securely
  - Anticipating and evaluating changes to your information system or network
  - Maintaining logs of authorized user's activity and keeping an eye out for unauthorized access

Due Diligence of Third Party Vendors

- Interagency guidance was issued by the FDIC, OCC, and Federal Reserve on "Conducting Due Diligence on Financial Technology Companies:



Joint Statement on Heightened Cybersecurity Risk

- On January 16, 2020, Federal Financial Regulators Issued Updated Bulletin on Cybersecurity Risks
- **"Implementing and maintaining effective cybersecurity controls is critical to protecting banks from malicious activity, especially in periods of heightened risk"**
- Sound risk management for cybersecurity includes the following:
  - Response and Resilience Capabilities
  - Authentication
  - System Configuration

Computer-Security Incident Notification Rule

- The Computer-Security Incident Notification Rule was published November 23, 2020

FIRST - Does this rule apply to me?

- Applies to entities regulated by the OCC, Federal Reserve, and FDIC
- Does not apply to state regulated entities or credit unions

SECOND - What does the Rule require?

1. Financial Institutions must notify their primary regulator within 36 hours after the bank has determined that a *computer security incident* that rises to the level of a notification incident has occurred

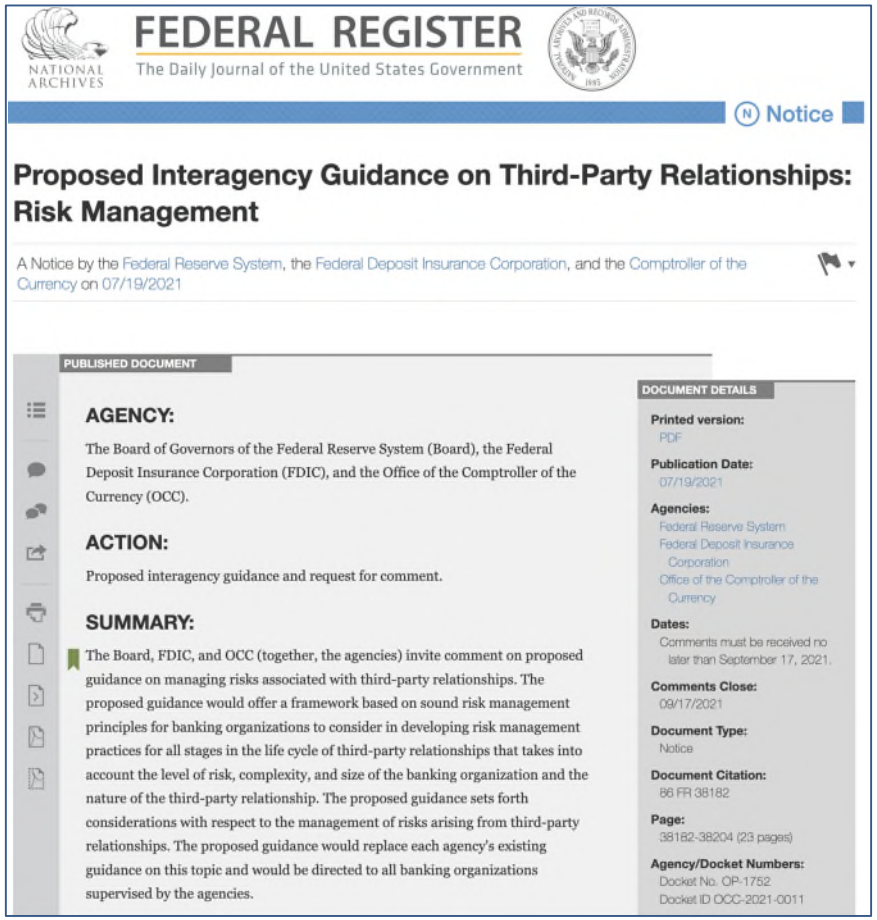
2. Financial Institutions must provide at least one bank-designated point of contact at each affected customer bank as soon as possible when it determines it has experienced a *computer-security incident* that has materially disrupted or degraded, or is reasonably likely to disrupt or degrade, covered services provided to the bank for four or more hours

THIRD - What is a *computer security incident*?

An occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits

Proposed Interagency Guidance on Third Party Relationships

- Proposed in July 2021 and has never been finalized
- Focus on a risk-based approach to vendor management
- Five steps to a risk-based third party vendor management program
    1) Appropriate Planning
    2) Due Diligence and Third Party Selection
    3) Contract Negotiation
    4) Ongoing Monitoring
    5) Termination of the Third-Party Relationship



FEDERAL REGISTER
The Daily Journal of the United States Government

Notice

Proposed Interagency Guidance on Third-Party Relationships: Risk Management

A Notice by the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Comptroller of the Currency on 07/19/2021

PUBLISHED DOCUMENT

AGENCY:

The Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC).

ACTION:

Proposed interagency guidance and request for comment.

SUMMARY:

The Board, FDIC, and OCC (together, the agencies) invite comment on proposed guidance on managing risks associated with third-party relationships. The proposed guidance would offer a framework based on sound risk management principles for banking organizations to consider in developing risk management practices for all stages in the life cycle of third-party relationships that takes into account the level of risk, complexity, and size of the banking organization and the nature of the third-party relationship. The proposed guidance sets forth considerations with respect to the management of risks arising from third-party relationships. The proposed guidance would replace each agency's existing guidance on this topic and would be directed to all banking organizations supervised by the agencies.

DOCUMENT DETAILS

Printed version: PDF
Publication Date: 07/19/2021
Agencies: Federal Reserve System; Federal Deposit Insurance Corporation; Office of the Comptroller of the Currency
Dates: Comments must be received no later than September 17, 2021.
Comments Close: 09/17/2021
Document Type: Notice
Document Citation: 86 FR 38182
Page: 38182-38204 (23 pages)
Agency/Docket Numbers: Docket No. OP-1752; Docket ID OCC-2021-0011

Updates to the FFIEC Cyber Resource Guide

- An October 6, 2022, update to the Cyber Resource Guide replaced 2018 guidance
  - The Guide includes programs and tools for financial institutions to use in meeting their security control objectives and to prepare to respond to cyber incidents
  - New focus on ransomware and malware attacks

- Updates the Resource Guide for Assessment, Exercise, Information Sharing, and Response and Reporting Categories

- New Ransomware Specific Resources

U.S. Treasury Report on Bank-FinTech Partnerships

- A November 2022 U.S. Treasury Report on Bank-FinTech partnerships highlighted benefits and concerns associated with these partnerships.

Benefits	Concerns
• New Business Models • New Technology • New Consumer Benefits	• Regulatory Arbitrage • Prudential Concerns • Inability to Draw Line between Commerce and Banking • Reliability (Service Levels) and Fraud • Data Privacy and Security • Bias and Potential Discrimination Particularly Related to AI-based Systems • Failure to Review Consumer Ability to Repay or Potential for Exploitation

Important Considerations for Board Members and Executive Management

- FTC has provided guidance emphasizing the importance of data security for board members.
- The FTC has continued to challenge allegedly deceptive or unfair conduct related to companies' data security practices. A few recent examples include settlements with SkyMed International, Zoom, and Tapplock.

Each settlement required, amongst other things:

- ❑ Notice to consumers regarding the incident,
- ❑ An Information Security Program
- ❑ Third-Party Information Security Assessments
- ❑ Annual Certification of Compliance with the Order
- ❑ Compliance report and notices

Recommendations for Board Members and Executive Management

- Five Recommendations for Boards of Directors (and Senior Management)

1. **Make Data Security a Priority**
   - Build a team of stakeholders from across your organization
   - Establish board-level oversight
   - Hold regular security briefings
2. **Understand the Cybersecurity Risks and Challenges your organization faces**
3. **Don’t Confuse Legal Compliance with Security**
4. **Focus on More than Just Prevention**
5. **Learn from Mistakes (yours and others’)**

Applicability Global & State Privacy Laws

- European Global Data Protection Regulation
- U.S. state data protection laws (thus far, California, Virginia, Colorado, Utah, Connecticut, and Nevada) provide carve-outs for the GLBA and FCRA.
  - These exemptions function in different ways: applying to types of entities, uses of certain data, and types of data. It is important to understand which laws apply and in which contexts.
  - There may be instances where an exemption *only partially* applies to a businesses data practices.
    - For example, where a business collects information from an individual that is *not* applying for a financial product or service (e.g., via website interactions, newsletters, contests, or other "lite" user activities), such information may fall outside of the scope of the GLBA and into the scope of the CCPA/CPRA.
    - GLBA and FCRA don't govern the collection of information from, or about, a business's employees and business-to-business ("B2B") contacts, which would be governed by CCPA/CPRA.
- Consider other global laws being enacted (e.g., Brazil General Data Protection Law)

Covered Acts

Q8. What acts are covered?	GDPR	CCPA	CPRA	VCDPA	CPA
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction	Any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means	Any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means	Any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data	The collection, use, sale, storage, disclosure, analysis, deletion, or modification of personal data and includes the actions of a controller directing a processor to process personal data
Selling	Not specifically defined	Selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration	Selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration	Exchange of personal data for monetary consideration	Exchange of personal data for monetary or other valuable consideration

https://assets.bbhub.io/bna/sites/7/2021/12/Comparison-Table-Privacy-Law-FAQs.pdf

Covered Acts

	GDPR	CCPA	CPRA	VCDPA	CPA
Q8. What acts are covered? (continued)					
Dark Patterns	Not specifically defined	Not specifically defined	A user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation	Not specifically defined	A user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice
Targeted Advertising	Not specifically defined	Not specifically defined	"Cross-context behavioral advertising": the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly branded website, application, or service with which the consumer intentionally interacts	Displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests	Displaying to a consumer an advertisement that is selected based on personal data obtained or inferred over time from the consumer's activities across nonaffiliated websites, applications, or online services to predict consumer preferences or interests
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements	Not specifically defined	Any form of automated processing of personal information, as further defined by regulations, to evaluate certain personal aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements	Any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements	Any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements

https://assets.bbhub.io/bna/sites/7/2021/12/Comparison-Table-Privacy-Law-FAQs.pdf

Individual Rights

	GDPR	CCPA	CPRA	VCDPA	CPA
Q9. What rights are granted to individuals?					
Notice	Yes	Yes	Yes	Yes	Yes
Access	Yes	Yes	Yes	Yes	Yes
Correct	Yes	No	Yes	Yes	Yes
Object / Opt-Out	Yes, under Art. 21	Yes	Yes	Yes	Yes
Limit use	Yes, under Art. 18	No	Yes, for sensitive information	No	No
Delete / Erasure	Yes	Yes	Yes	Yes	Yes
Data portability	Yes	Yes	Yes	Yes	Yes
Free exercise of enumerated rights (Nondiscrimination)	Art. 23 permits Union or Member State law to restrict by way of a legislative measure the scope of data subject rights under certain circumstances	Yes	Yes	Yes, but also extends to state and federal laws that prohibit unlawful discrimination against consumers	No; CPA's duty to avoid unlawful discrimination only prohibits a controller from processing person data in violation of state and federal laws that prohibit unlawful discrimination against consumers
Private right of action	Yes, via Art. 79	Limited	Limited	No	No
Other redress	Yes, via Supervisory Authority	Yes, via AG	Yes, via California Privacy Protection Agency	Yes, via appeal, then AG	Yes, via appeal, then AG

https://assets.bbhub.io/bna/sites/7/2021/12/Comparison-Table-Privacy-Law-FAQs.pdf

Other Business Obligations

- Transparency
- Explicit purpose
- Data minimization
- Consent (explicit vs. implicit)
- Data Protection Assessments
- Record keeping
- Data Protection Officer
- Data security
- Breach noticfication

Presenter Biographies

DOWSE BRADWELL "BRAD" RUSTIN IV

Brad Rustin chairs the firm's Financial Services Regulatory Practice. He began his career as a litigator focusing on consumer financial services litigation and defense of regulatory claims against chartered and non-chartered financial institutions, finance entities, and money services business. Following in the wake of the fiscal crisis, he began working with financial institutions, state-licensed lenders, money transmitters, non-traditional lenders, check cashers, and mortgage brokers on issues of regulatory compliance. Brad is a Certified Anti-Money Laundering Specialist (CAMS) by ACAMS and a Certified Regulatory Compliance Manager (CRCM) by the American Bankers Association. He also serves as an expert witness of matters relating to financial regulations and compliance.

MALLORY ACHESON, CIPM

Mallory Acheson focuses on privacy and security compliance, technology transactions, and the intersection of data and electronic discovery issues. Mallory helps clients navigate domestic and internal privacy laws, including CCPA/CPRA, GDPR, TCPA, HIPAA, and GLBA. She assists clients in developing and executing compliance programs, privacy policies, data processing agreements, and related regulatory analysis.

ELIZABETH DONALDSON

Elizabeth Donaldson advises a variety of entities with regulatory and compliance matters related to the consumer finance industry, including state and federal consumer protection laws, regulation and licensing, anti–money laundering and Bank Secrecy Act compliance, and traditional and non–traditional lending. She assists clients throughout the lifecycle of product development as they strive to offer new and innovative products and services through both traditional and online channels. Elizabeth regularly works with banks, mortgage companies, consumer lenders, payments companies, auto lenders, and FinTech companies to develop compliance policies and procedures, review compliance with state and federal laws, and draft key contracts.

Moderator Biography

RICHARD B. LEVIN

Richard is chair of the FinTech and Regulation Practice and was one of the first lawyers to focus on the regulation of blockchain and digital assets. He is considered a thought leader in the FinTech space. Richard brings his experience as a senior legal and compliance officer on Wall Street and in London to bear in advising clients on corporate, FinTech, securities, and regulatory issues. A problem-solver by nature, he has been advising FinTech clients on legal and regulatory issues since the start of electronic trading in the late 1990s. His practice focuses on helping financial services and technology clients identify and address regulatory issues as they build their businesses.

Richard's practice focuses on the representation of early stage and publicly traded companies in the FinTech space, including investment banks, broker-dealers, investment advisers, peer-to-peer lending platforms, digital currency trading platforms, alternative trading systems (ATSs), exchanges, and custodians. He represents these firms before the U.S. Securities and Exchange Commission (SEC), the U.S. Commodity Futures Trading Commission (CFTC), the Financial Industry Regulatory Authority (FINRA), the U.S. Department of the Treasury, Office of the Comptroller of the Currency (OCC), state regulators, and Congress. Richard has represented clients before regulators in Australia, Canada, France, Germany, Hong Kong, Ireland, Japan, Singapore, South Korea, and the United Kingdom. His current and past clients include leading national financial institutions, multinational financial services holding companies, leading firms in the FinTech space, and institutions engaging in global investment banking, investment management, securities, and other financial services with institutional clients.

Richard has been identified by Chambers and Partners as one of the leading lawyers in the Blockchain and Cryptocurrencies category since the inception of the category. He has been recognized by Chambers for his knowledge on regulatory matters, great relationships with regulators, for helping clients push the boundaries of the FinTech sector, and for his advice on matters such as broker-dealer licensing and alternative trading systems. Richard is routinely quoted by leading publications including Bloomberg, the New York Times, Reuters, and the Wall Street Journal and is a frequent speaker at conferences around the world on the regulation of FinTech, blockchain, and digital assets.

Contact Details

To learn more about our FinTech and Regulation practice, or to contact a member of our team, click here or visit our website at nelsonmullins.com.

To learn more about this presentation, please call:

Richard B. Levin
1400 Wewatta Street
Suite 500
Denver, CO 80202
Tel. 303.583.9929
richard.levin@nelsonmullins.com

Brad Rustin
2 W. Washington Street
Suite 400
Greenville, SC 29601
Tel. 864.373.2320
brad.rustin@nelsonmullins.com

Mallory Acheson
150 Fourth Avenue North
Suite 1100
Nashville, TN 37219
Tel. 615.664.5378
mallory.acheson@nelsonmullins.com

Elizabeth Donaldson
2 W. Washington Street
Suite 400
Greenville, SC 29601
Tel. 864.373.2248
liz.donaldson@nelsonmullins.com

About This Publication

- Nelson Mullins provides this material for informational purposes only.
- The material provided herein is general and is not intended to be legal advice.
- Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues.
- Receipt of this material does not establish an attorney-client relationship.
- Nelson Mullins is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.