Cybersecurity, Privacy and Communications Webinar: Financial Privacy Primer

March 23, 2017

Heather Zachary, Partner
Nicole Ewart, Senior Associate

WILMERHALE

Attorney Advertising

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Speakers

Heather Zachary, Partner

Nicole Ewart, Senior Associate

Webinar Guidelines

- Participants are in listen-only mode
- Submit questions via the Q&A box on the bottom right panel
- Questions will be answered as time permits
- Offering 1.0 CLE credit in California and New York*
- WebEx customer support: +1 888 447 1119, press 2

**WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional CLE credit in New York. This program, therefore, is being planned with the intention to offer CLE credit for experienced New York attorneys only. Attendees of this program will be able to claim England & Wales CPD for this program. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Attendees requesting CLE credit must attend the entire program.*

Agenda

- Gramm-Leach-Bliley Act
  - Privacy Rule
  - Exceptions and Use Limitations
  - Information Security Safeguards
  - Enforcement
- Right to Financial Privacy Act
- Fair Credit Reporting Act
  - Consumer Reports and Consumer Reporting Agencies
  - Permissible Purposes, Employment Use, and Marketing
  - Red Flags Rule
- Enforcement and Litigation Trends

The Gramm-Leach-Bliley Act

History of the Gramm-Leach-Bliley Act

Part V of the law addressed financial privacy and security (15 U.S.C. § 6801 *et seq.*)

- Enforcement and rulemaking responsibility for the GLBA privacy provisions was previously shared by 8 federal agencies: FDIC, FRB, FTC, NCUA, OCC, OTS, SEC, and CFTC.

Title X of the Dodd-Frank Act transferred rulemaking authority for the GLBA ***privacy*** provisions to the CFPB.

- The SEC, CFTC, and FTC retain rulemaking authority for the privacy provisions with respect to certain institutions.
- Several federal agencies retain authority with respect to GLBA ***security*** provisions.

GLBA Privacy Rule

- The Gramm-Leach-Bliley Act and its implementing regulations impose a range of ***privacy*** obligations on financial institutions that exceed those imposed on most other types of businesses.
- GLBA regulates the sharing of **"nonpublic personal information"** about **"consumers"** and **"customers"** with **"nonaffiliated third parties"**
- Consumer v. Customer
  - **Consumer:** An individual who obtains a financial product or service that is used primarily for personal, family, or household purposes
  - **Customer:** Consumer with whom the institution has a continuing relationship, under which the institution provides one or more financial products or services

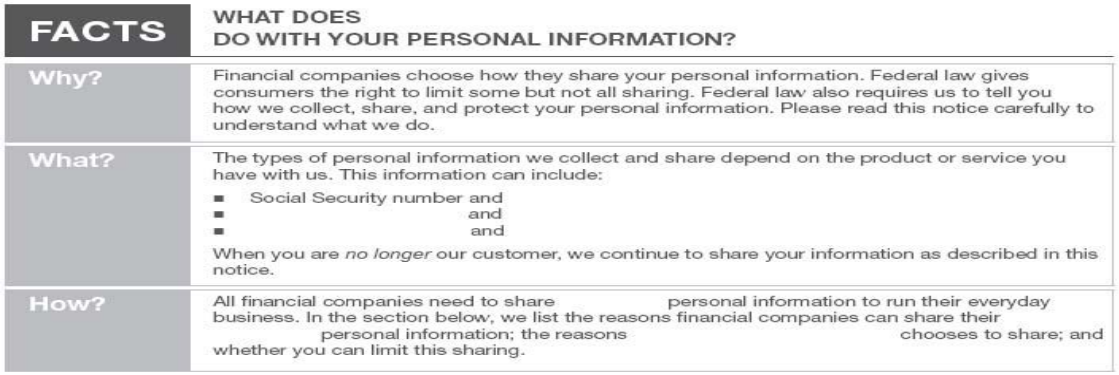
GLBA Privacy Rule: Covered Information

- **"Nonpublic personal information"**:
  - Consumer information (e.g., name, address, income, SSN)
  - Transactional information (e.g., account numbers, payment history)
  - Other information (e.g., court records, some online "cookie" information)
- Includes even the fact that a person is or was a customer
- Does not include some information that is lawfully made "publicly available"

GLBA Privacy Rule

Unless an exception applies, a financial institution may not disclose any nonpublic personal information about a consumer to a nonaffiliated third party unless:

- The financial institution provides an initial notice of its privacy practices;
- The financial institution has provided an opt out notice;
- The consumer is given a reasonable opportunity to opt out; and
- The consumer does not opt out. (12 CFR 1016.10)



FACTS	WHAT DOES DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ▪ Social Security number and ▪ and ▪ and When you are *no longer* our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share personal information to run their everyday business. In the section below, we list the reasons financial companies can share their personal information; the reasons chooses to share; and whether you can limit this sharing.

GLBA Privacy Rule: Privacy Notices

- Customers:
  - You must give customers an **initial privacy notice** when you establish the customer relationship (12 CFR 1016.4)
  - If you share NPI with certain nonaffiliated third parties, you also must give customers an **opt-out notice**, a reasonable way to opt out, and enough time to opt out before disclosing NPI
  - **Annual notice** requirement thereafter (in some cases)

GLBA Privacy Rule: Notice Safe Harbor

Financial institutions may rely on the model privacy form as a safe harbor to comply with the GLBA notice requirements.

Rev. [insert date]

FACTS	WHAT DOES [NAME OF FINANCIAL INSTITUTION] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of financial institution] share?	Can you limit this sharing?
For our everyday business purposes—such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes—to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes—information about your transactions and experiences		
For our affiliates' everyday business purposes—information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

To limit our sharing	■ Call **[phone number]**—our menu will prompt you through your choice(s) or ■ Visit us online: **[website]** **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [website]

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of financial institution] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of financial institution] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account—unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

GLBA Privacy Rule: Annual Privacy Notices

An annual notice is required once every 12 consecutive months during the continuation of the customer relationship. (12 CFR 1016.5)

- Not required for former customers.

Alternative delivery method (posting on website) for annual privacy notices to customers available if the financial institution satisfies certain requirements listed in the regulation. (CFPB only; 12 CFR 1016.9)

FAST Act Amendment to GLBA in December 2015 added an exception to the annual disclosure requirement in certain circumstances.

- Does not apply to the initial notice
- Does not change FCRA opt-out notice requirement
- Does not alter state financial privacy law notice requirements

GLBA Privacy Rule: Exceptions

- Exception from Notice ***and*** Opt-Out Requirements
  - Information-sharing necessary for effecting, administering, or enforcing a transaction requested or authorized by a consumer
  - Sharing with the consent of, or at the direction of, the consumer
  - Sharing for purposes of (among other things) preventing fraud, protecting confidentiality/security of records, ensuring institutional risk control, facilitating a merger or similar transaction, responding to judicial process or investigation, or complying with federal, state, or local laws
- Exception from Opt-Out Requirement
  - Disclosures to third-party service providers
  - Marketing financial products or services offered through a "joint agreement" with one or more other financial institutions
  - Such sharing is subject to compliance with specific contractual requirements designed to protect nonpublic personal information

GLBA Privacy Rule: Reuse and Re-disclosure Limits

If an entity receives NPI from a nonaffiliated financial institution, its disclosure and use of the information is limited.

If received under an exception, it can disclose the NPI to:

- The affiliates of the financial institution from which it received the information;
- Its own affiliates; and
- Pursuant to a Section 14 or 15 notice and opt out exception

(12 CFR 1016.11)

If not received under a Section 14 or 15 exception, **use** for your own purposes is permitted, but **disclosure** is restricted. (12 CFR 1016.11(b))

GLBA Violations

Federal financial regulators may bring enforcement actions for violation of the GLBA privacy provisions

There is **no private right of action** for violation of the GLBA

- Some state analogues *do* have private rights of action

State attorneys general also can also enforce the GLBA

State Analogue: California's SB1

- Not preempted by federal statute or regulations
- Opt-***in*** for sharing information with nonaffiliated third parties
- Opt-***out*** for some sharing of information with affiliated parties
- Special customer notice form available
- Other states have similar laws, and many are outdated

Information Security Safeguards

Security Safeguards

The GLBA also requires federal financial regulators and the FTC to establish standards for financial institutions relating to **administrative, technical, and physical safeguards** for consumer information.
(15 U.S.C. §§ 6801(b), 6805(b)(2))

- The federal banking agencies (Fed, FDIC, OCC, OTS, and NCUA) promulgated the **Interagency Guidelines Establishing Information Security Standards** (66 Fed. Reg. 8616)
- The FTC promulgated the **Safeguards Rule** (Standards for Safeguarding Customer Information) (16 CFR 314)
- The SEC implemented **Procedures to Safeguard Customer Records and Information** (17 CFR 248.30)

Dodd-Frank expressly carved out the GLBA's data security provisions from the CFPB's jurisdiction.

Interagency Guidelines

The guidelines apply to a wide range of financial institutions that are regulated by the Fed, FDIC, OCC, OTS, and NCUA

They govern "customer information" maintained by or on behalf of such financial institutions

Entities are required to establish a **Written Information Security Program** appropriate to the size and complexity of the entity and the nature and scope of its activities, designed to:

- Ensure the security and confidentiality of customer information
- Protect against any anticipated threats or hazards to the security or integrity of such information, and
- Protect against unauthorized access to or use of such information that would result in substantial harm or inconvenience to any customer

Interagency Guidelines

- Board of directors' involvement
- Risk assessment
- Risk management and control
- Oversight of service providers
- Written security incident response plan
- Periodic updating

Interagency Guidance – Incident Response

Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (70 Fed. Reg. 15736)

- A risk-based response program is a key part of a financial institution's information security program
- At a minimum, a financial institution's incident response program must contain procedures for:
  - Assessing the nature and scope of the incident and what systems and customer information was accessed or misused
  - Notifying the primary federal regulator in cases of incidents involving **sensitive customer information**
  - Notifying appropriate law enforcement authorities and filing SARs, where appropriate
  - Taking steps to contain and control the incident
  - Notifying affected customers when warranted

Interagency Guidance – Incident Response

- Customer notice is required *only* where there has been unauthorized access to *sensitive customer information* and misuse of the information has occurred or is reasonably possible.
- Sensitive customer information means:

Any of these		Any of these	
Name	In conjunction with:	Social Security Number	Driver's License Number
Address		Account Number	Credit or Debit Card Number
Telephone Number		Personal Identification Number	Password

- It also includes any combination of information allowing access to a consumer's account (such as an online ID and password).
- When customer notice is required, the Guidance sets forth the minimum contents of the notice.
- Notice to *regulators* is required in additional circumstances: unauthorized access to sensitive customer information suffices. There is *no risk trigger*

FTC and SEC Safeguards Rule

Similar to but less prescriptive than the Interagency Guidelines.

- Each financial institution (subject to the FTC's jurisdiction) must develop a **written information security program** appropriate to its size and the complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue.
- SEC regulated entities required to **adopt written policies and procedures** addressing administrative, technical, and physical safeguards for the protection of customer records and information

Safeguards Enforcement

The FTC has brought more than a dozen actions against institutions under its jurisdiction for violation of the Safeguards Rule.

The SEC has been increasingly active in enforcement of its GLBA data security provisions.

- Imposed a $1 million fine on Morgan Stanley in June 2016 after 730,000 Morgan Stanley customer accounts were compromised when a former employee who downloaded the data to a personal account was hacked by a third party
- Broker-dealer Craig Scott Capital paid $100,000 to the SEC in April 2016 for its employees' use of personal email addresses to conduct business involving sensitive customer data (case based on risk of security incident, not an actual incident)

Although the CFPB lacks jurisdiction for data security under the GLBA, the CFPB has used its UDAAP (unfair, deceptive, and abusive acts and practices) powers to participate in data security supervision, rulemaking, and enforcement.

- The CFPB filed its first data security enforcement action in March 2016 (*Dwolla, Inc.*).

Right to Financial Privacy Act

Right to Financial Privacy Act

- Restricts ***government*** access to customer records held by financial institutions, but requires that financial institutions take steps to ensure compliance.
- Requires certain procedures to be followed before records are disclosed, often including notice to the consumer and an opportunity to object to object to the disclosure.
- In many cases, the government provides a certificate of compliance to the financial institution, and that certificate conveys immunity from liability for ***good-faith*** violations of the Act.

Responding to Government Data Requests

- There are *many* exceptions to the RFPA's requirements.
  - Examples include requests related to taxes, national security, bank examinations, and grand jury proceedings
  - In some cases, the exception is merely to the notice requirement, while in others the exception encompasses the certification requirement as well
- RFPA applies only to ***federal*** government requests, not requests from state or local governments or private parties. But many similar laws exist on the state level.
- RFPA protects only individuals or partnerships of five or fewer individuals.

Fair Credit Reporting Act

Fair Credit Reporting Act

- Regulates "**consumer reporting agencies**" (CRAs) and those who use or furnish information for "**consumer reports**"
- A **consumer report** is communication of information: (i) bearing on credit worthiness, credit standing, credit capacity, character, reputation, personal characteristics, or mode of living, (ii) that is collected or used for purposes of establishing eligibility for credit, insurance, or employment, or for certain other purposes
- Communicating "consumer report" information can subject an entity to regulation as a "consumer reporting agency"
- A **consumer reporting agency** is:
  - A person that regularly engages in assembling or evaluating information on consumers for the purpose of furnishing consumer reports to third parties.

Consumer Reports

"**Consumer**" includes only natural persons, not artificial entities.

- Reports about corporations, associations, or other collective entities are not reports about a "consumer" and thus are not subject to FCRA.

Communications about more than just consumer credit information can constitute a "consumer report."

- Driving record
- Employment record
- Criminal history
- Education
- Licenses held
- Rental history

Such information sheds light on the consumer's character, general reputation, personal characteristics, or mode of living.

Duties of Consumer Reporting Agencies

Consumer reporting agencies must (among other things):

- Have **permissible purposes** to furnish consumer reports;
- Take certain actions relating to identity theft;
- Avoid supplying obsolete adverse information;
- Adopt reasonable procedures to assure privacy and accuracy of consumer reports;
- Provide only limited disclosures to governmental agencies;
- Provide consumers certain disclosures upon request at no cost, or for a reasonable charge;
- Follow certain procedures if a consumer disputes the completeness or accuracy of any item of information contained in his or her file;
- Follow certain procedures in reporting public record information for employment purposes or when reporting adverse information other than public record information in investigative consumer reports.

Exception: Transaction or Experience Info

- Reports limited ***solely*** to transactions or experiences between the consumer and the entity making the report are ***not*** consumer reports.
  - First-hand reports of a consumer's performance (e.g., an employer describing an employee's job performance)
  - Lab reports (e.g., drug test results provided by a lab directly to an employer)
  - Personal observations (e.g., an investigator who records events)
  - Creditor information (e.g., information about a consumer's repayment of a debt, or a list provided by a creditor of its customers who have account balances of >$10,000 would constitute transaction or experience info when provided by the creditor)
- However, a report by a creditor of ***application information*** supplied by the consumer (such as a list of his or her assets and liabilities) ***is not the creditor's "transaction or experience" information*** because it includes information about the consumer's transactions with entities other than the creditor.

Affiliate Marketing

- Information obtained from affiliates cannot be used to make a solicitation for marketing purposes to a consumer about an entity's products or services, unless:
  - The consumer has been given clear and conspicuous notice of the sharing for affiliate marketing purposes;
  - The consumer has been provided an opportunity and a simple method to opt out; and
  - The consumer has not opted out.
- The notice can be combined with other notices such as the GLBA privacy notice. 12 CFR 1022.23(b)

Permissible Purposes

CRAs may furnish consumer reports *only* for permissible purposes and no other purpose. These include:

- Order of a court, or a subpoena issued in connection with federal grand jury proceedings.
  - A subpoena is not an order of a court unless it is signed by a judge
  - EXCEPTION: Internal revenue summons
- Written consent from the consumer
- In connection with a credit transaction involving the consumer
- For review or collection of an account
- For employment purposes
- In connection with the underwriting of insurance involving the consumer
- In connection with a consumer's eligibility for a license or other benefit granted by a governmental instrumentality
- Legitimate business need in connection with a business transaction initiated by the consumer (e.g., apartment rental)
- In connection with the assessment of child support obligations

Permissible Purposes - Employment

To furnish a consumer report for employment purposes, the CRA must obtain a certification from the user (employer) stating that the user:

1. Has obtained the consumer's consent
2. Will provide the consumer with a copy of his or her report and a summary of rights under the FCRA before taking adverse action, and
3. Will not use the report to violate employment opportunity laws

Employment Purposes - Consent

Persons seeking a consumer report for employment purposes must:

1. Make a clear and conspicuous disclosure in writing to the consumer before the report is procured or caused to be procured, ***in a document that consists solely of the disclosure***, that a consumer report may be obtained for employment purposes; and
2. Obtain from the consumer authorization in writing for the procurement of the report by that person (the authorization may be made on the disclosure form)

Employment Purposes – Refusal to Consent

FCRA does not prohibit an employer from taking an adverse action against an employee or applicant who refuses to authorize the employer to procure a consumer report.

Employment Purpose – Adverse Action

Pre-adverse Action Notice

- **Before** taking any adverse action based on a consumer report, employers must provide the consumer with a copy of the report and a written summary of consumer rights under the FCRA.
- There is no specific period of time an employer must wait after providing the pre-adverse action notice and before taking adverse action against the consumer. Some reasonable period of time must elapse, but the minimum length will vary depending on the particular circumstances involved.

Notice of Adverse Action

- Oral, written, or electronic notice of adverse action
- Name, address, and phone number of the CRA
- Statement that the CRA did not make the decision to take the adverse action and is unable to provide specific reasons for the action
- Notice of the consumer's right to obtain a free file disclosure from the CRA, and to dispute with the CRA the accuracy or completeness of any information in the report
- Disclose any numerical credit score that contributed to the adverse action.

Other Users of Consumer Reports

- Users may obtain consumer reports only for permissible purposes.
- Users must certify the purposes for which the consumer report is sought and certify that the consumer report will be used only for the stated permissible purpose.
- Users must notify the consumer when an adverse action is taken in whole or in part on the basis of a consumer report.
- Users must provide risk-based pricing notices in certain cases where a decision to offer materially less favorable credit terms is based in whole or in part on a consumer report.
- Users must identify the consumer reporting agency that provided the report in order to permit the accuracy and completeness of the report to be verified or contested by the consumer.

Duties of Information Furnishers

- Entities that ***furnish*** information to consumer reporting agencies have obligations as well.
  - Furnishers may not supply information to CRA if they know, or have reasonable cause to believe, that the information is inaccurate.
  - Consumers may dispute directly with furnishers the accuracy of information supplied to a CRA. FCRA imposes specific procedural and timing requirements on furnishers in the event of such a dispute, including investigation and correction obligations.
- Financial institutions that extend credit and that regularly and in the ordinary course of business furnish information to CRAs must provide clear and conspicuous written notice to customers if furnishing negative information.
  - The CFPB provides a model disclosure that furnishers may use

"Red Flag" Identity Theft Rules

- Fair and Accurate Credit Transactions Act (FACTA)
- "Financial institutions" and "creditors" must perform periodic risk assessments to determine if they have "covered accounts"
- Entities that offer or maintain "covered accounts" are required to establish and comply with a written identity theft program

Identity Theft Program Requirements

- Identify the red flags that may occur
  - Suspicious documents
  - Alerts from a third party
  - Suspicious account activity
- Detect identified red flags
  - Identity verification and authentication
  - New versus existing accounts
- Respond appropriately when a red flag has been detected
  - Contact customer or change password
  - Cease contact or refuse to open account
  - Contact law enforcement / file suspicious activities report ("SAR")
- Update the plan to address new threats

Disposal of Records

- FCRA requires any person that maintains or otherwise possesses consumer information, or any compilation of consumer information, that is derived from consumer reports to properly dispose of any such information.
- The person must take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

FCRA Litigation Trends

- Compared to 2015, FCRA lawsuits were up 8.4% in 2016.
- Over the last few years, a number of class action suits have involved claims of inadequate disclosure and authorization for background checks during the hiring process.
  - *In re Michaels Stores, Inc., Fair Credit Reporting Act (FCRA) Litig* (D.N.J. Jan. 24, 2017) (alleging FCRA disclosure in middle of online application, but dismissed on grounds of insufficient injury in fact to support standing)
  - *Hargrett v. Amazon.com* (January 30, 2017) (alleging FCRA disclosure and consent was included with liability release and other state law notices; withstood motion to dismiss on standing ground because concrete injury shown through invasion of privacy, informational harm, and risk of harm)
- Some courts have found violations are "willful," exposing the employer to statutory penalties, punitive damages and attorney's fees awards.

CFPB Focus on Furnishers

In its recent bulletins and Supervisory Highlights publications, the CFPB has reiterated the importance of FCRA compliance for a broad spectrum of FCRA-regulated entities and specifically highlighted its interest in and supervision of furnishers of information.

- The focus on furnishers has been a consistent trend over the past few years.
- In 2015, the CFPB brought a number of strict enforcement actions that resulted in large fines, including a $6.4 million fine against CarHop, one of the country's biggest "buy-here, pay-here" auto dealers, and its affiliated financing company, Universal Acceptance, for providing "damaging, inaccurate consumer information to credit reporting companies."

cfpb Consumer Financial Protection Bureau

Questions?

Heather Zachary, Partner
heather.zachary@wilmerhale.com

Nicole Ewart, Senior Associate
nicole.ewart@wilmerhale.com

**WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional CLE credit in New York. This program, therefore, is being planned with the intention to offer CLE credit for experienced New York attorneys only. Attendees of this program will be able to claim England & Wales CPD for this program. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Attendees requesting CLE credit must attend the entire program.*