Ballard Spahr LLP

Minneapolis Card Issuers Workshop

May 14, 2019

Ballard Spahr LLP

Ballard Spahr LLP

Vendor Risk Management for Bank Agreements: Points to Consider and Avoiding "Teachable Moments"

Glen P. Trudel
Partner
302.252.4464
trudelg@ballardspahr.com

Ron K. Vaske
Partner
612.371.3215
vaske@ballardspahr.com

Judy M. Mok
Of Counsel
646.346.8008
mokj@ballardspahr.com

Ballard Spahr LLP

Ballard Spahr LLP

Importance of Vendor Management in Bank Partnership Arrangements

Ballard Spahr LLP

Importance of Vendor Management in Bank Partnership Arrangements

- OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," issued October 30, 2013
- Supplemented by OCC Bulletin 2017-21, "Frequently Asked Questions to Supplement OCC Bulletin 2013-29"

Ballard Spahr LLP

Importance of Vendor Management in Bank Partnership Arrangements

- Federal Reserve SR 13-19/CA 13-21, "Guidance on Managing Outsourcing Risk" issued on December 5, 2013

Ballard Spahr LLP

Importance of Vendor Management in Bank Partnership Arrangements

- FDIC FIL 44-2008, "Guidance for Managing Third Party Risk" issued on June 6, 2008
- FDIC FIL 50-2016, Proposed "Examination Guidance for Third-Party Lending" proposed on July 29, 2016

Ballard Spahr LLP

Critical Activities

Regulators expect more comprehensive and rigorous bank oversight and management of 3rd party relationships that involve "critical activities"

Ballard Spahr LLP

Critical Activities

- Significant risk to bank if 3rd party fails to meet expectations
- Significant customer impact
- Requires significant investment in resources to implement 3rd party relationship and manage risk
- Major impact on bank operations if alternate 3rd party needed or outsourced activity needs to be brought back in-house

Ballard Spahr LLP

Contractual Provisions

- Banks are expected to be prudent in choosing appropriate third party service providers and monitoring their performance, beginning with contract negotiations
- The Agencies expect to see certain types of contractual provisions in banks' agreements with their service providers

**See Appendix 1 for full list*

Ballard Spahr LLP

Contractual Provisions

- Some key contractual topics described in the Agency Guidance include:
  - Responsibility for Compliance with Applicable Laws
  - Indemnification
  - Default and Termination
- Discussion in context of:
  - Co-Brand Credit Card Program Agreements
  - Bank Sponsorship Agreements

Ballard Spahr LLP

Practical Tips for Co-Brand Agreements:
Responsibility for Compliance with Applicable Laws and Regulations

- **Guidance:**

Ensure bank has right to monitor on an ongoing basis third party's compliance with applicable laws, regulations and policies and requires remediation if issues arise.

- **Practical Tips:**
  - ✓ When drafting contract, consider distinguishing between "Bank Applicable Law" vs "Service Provider Applicable Law".
  - ✓ Delineate applicable laws that are unique to a party that would govern that party's provision of services or activities under the agreement.
  - ✓ A party should be responsible for instructing the other party to comply with its set of applicable laws if the two sets of applicable laws relate to different industries and are different in scope.

Ballard Spahr LLP

Practical Tips for Sponsorship Agreements:
Responsibility for Compliance with Applicable Laws and Regulations

- **Guidance:**

Ensure bank has right to monitor on an ongoing basis third party's compliance with applicable laws, regulations and policies and requires remediation if issues arise.

- **Practical Tips:**
  - ✓ Manager is bank's agent/service provider.
  - ✓ Manager typically has contractual responsibility for compliance.
  - ✓ Bank has legal responsibility for compliance, even if allocated to Manager in contract.
  - ✓ Bank should have final authority re: determinations of law.
  - ✓ Third party audit may be appropriate (e.g., processor oversight).
  - ✓ Bank's broad monitoring and approval authority over media and performance.

Ballard Spahr LLP

Practical Tips for Co-Brand Agreements: Indemnification/Limits on Liability

- **Guidance:**

Specify extent of bank liability for third party failure to perform, assess indemnification clauses that require bank to hold third party harmless from liability, and consider whether proposed limit is in proportion to the amount of loss bank might experience because of third party's failure to perform or comply with applicable laws.

- **Practical Tips:**
  - ✓ May have more success in negotiating with a party by asking such party to take on risks that are within its control.
  - ✓ Which party is engaging in the activities that are more likely to incur liability?
  - ✓ Which party has more consumer facing risk and liability?
  - ✓ Are there risks of class action lawsuits?

Practical Tips for Sponsorship Agreements: Indemnification/Limits on Liability

- **Guidance:**

Specify extent of bank liability for third party failure to perform, assess indemnification clauses that require bank to hold third party harmless from liability, and consider whether proposed limit is in proportion to the amount of loss bank might experience because of third party's failure to perform or comply with applicable laws.

- **Practical Tips:**
  - ✓ Consider program economics
    - ✓ Which party receives fixed amount versus all excess revenue?
    - ✓ Which party owns portfolio upon termination of contract?
  - ✓ Which party receives the benefit of the activity incurring liability?
    - ✓ Illegal interest and fees
    - ✓ Unclaimed property
  - ✓ Bank cannot be indemnified for losses due to penalties (CMP).

Practical Tips for Co-Brand and Sponsorship Agreements: Termination Rights

- **Guidance:**

  Include "a provision that enables the bank to terminate the contract, upon reasonable notice and without penalty, in the event that the Agency formally directs the bank to terminate the relationship."

- **Practical Tips:**
  - ✓ Negotiate termination rights for changes in applicable law.
  - ✓ Define "applicable law" broadly to include not just statutes and regulations, but also regulatory guidance, orders and interpretations of governmental authorities.
  - ✓ Exit rights if there are material adverse effects on either party or on the overall bank partnership program *(e.g.,* reputational harm, litigation risks, change in law).

APPENDIX 1: Agency Guidance provides that banks' contracts with third party service providers should address the following topics:

1. Nature and Scope of Arrangement
2. Performance Measures or Benchmarks
3. Responsibilities for Providing, Receiving, and Retaining Information
4. The Right to Audit and Require Remediation
5. Responsibility for Compliance with Applicable Laws and Regulations
6. Cost and Compensation
7. Ownership and License
8. Confidentiality and Integrity
9. Business Resumption and Contingency Plans
10. Indemnification
11. Insurance
12. Dispute Resolution
13. Limits on Liability
14. Default and Termination
15. Customer Complaints
16. Subcontracting
17. Foreign-Based Third Parties
18. Agency Supervision

Ballard Spahr LLP

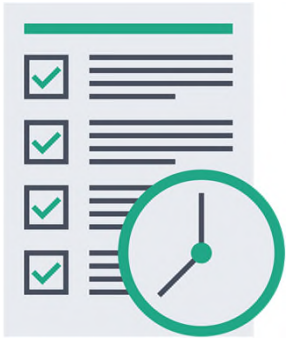
Vendor Risk Management: Avoiding Teachable Moments

Ballard Spahr LLP

Preparing for an Exam

Understand the type/ scope of exam

- Will third party programs/ relationships be a specific/central focus?
- What other areas of focus?
  How might the exam topics (laws/regs, products/ services…) intersect your organization's third party relationships?



Understand/anticipate regulators' priorities more broadly

- Communications from examiners
- Examination procedures
- Agency issuances
- Enforcement actions/trends
  Consider agencies in addition to your organization's primary federal regulator

Ballard Spahr LLP

Preparing for an Exam – Show & Tell

Coherently/cohesively put forth the (true!) "story" of your organization's third party program/risk management approach

Give attention to organization/format/flow /understandability

Document & include:

- Clear (and current/accurate!) policies/procedures with channels of reporting/responsibility
- Evidence of training on policies and procedures
- Evidence policies and procedures are actually being followed
- Evidence on management of third party relationships along the entire lifecycle
  - Information on processes for identifying risks, continuing oversight/monitoring, and obtaining/following up on monitoring results
- Documentation of how board of directors kept appropriately informed/involved

Preparing for an Exam – Managing Expectations

Establish clear team roles in gathering/providing info and for the entire exam process

- Are all team members on the same page?
- Who will need to be available and when?
- Who is appropriate to answer which questions?
- What information may need to be obtained from service providers?
- Can all follow-up information be provided in a timely manner to exam staff?

Avoiding Missteps & Mitigating Risk

"An organization can outsource the task, but not the responsibility."

- ✓ Own/embrace responsibility for compliance/risk management, including oversight
- ✓ Third party relationships can be tools to help your organization achieve its goals, but you ultimately remain responsible for setting the goals, as well as your own risk appetite, compliance strategies, etc.

What are the particular risks raised by particular third party relationships/ activities?

- ✓ Continue to assess this throughout third party relationship lifecycle
- ✓ Keep current on hot-button issues

Ensure policies and procedures are current/accurate and appropriate

- ✓ Informed by risk assessments, monitoring, etc.

Document, document, document

- ✓ And document some more

All phases of third party risk management lifecycle are important

- ✓ Consider phases that may warrant particular attention in a given relationship/circumstance
  - ✓ Monitoring is one phase where things have often gone awry

Ballard Spahr LLP

Avoiding Missteps & Mitigating Risks – Monitoring

Avoid treating monitoring as static

- ✓ See third party relationships as living/evolving relationships and monitoring as an iterative process
- ✓ Different types of monitoring may be appropriate for different types of third parties/activities and under different circumstances
- ✓ Monitoring should build on itself and inform further monitoring (as well as potential changes in relationship itself)

Avoid treating monitoring as done for the sake of monitoring

- ✓ What is your monitoring telling you? What are you doing in response?
- ✓ Should monitoring type/frequency change in response?
- ✓ Should something substantive about the relationship change?

Document, document, document

Ballard Spahr LLP

Teachable Moments – Regulatory Activity

Recent regulatory activity provides certain reminders for those responsible for third party vendor risk management

- **Wells Fargo Consent Orders** (CFPB Consent Order File No. 2018-BCFP-0001 and OCC Consent Order #2018-16) https://files.consumerfinance.gov/f/documents/cfpb_wells-fargo-bank-na_consent-order_2018-04.pdf and https://www.occ.gov/news-issuances/news-releases/2018/nr-occ-2018-41.html
- **National Credit Adjusters, LLC and Bradley Hochstein** (Consent Order File No. 2018-BCFP-0004) https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/bcfp_national-credit-adjusters_consent-order_2018-07.pdf
- **FDIC's FIL-19-2019 "Technology Service Provider Contracts" (April 2, 2019)** https://www.fdic.gov/news/news/financial/2019/fil19019.html

Ballard Spahr LLP

Teachable Moments – Consent Orders

Wells Fargo Bank, N.A. Consent Orders (April 20, 2018)

- CFPB determined that Wells violated the Consumer Financial Protection Act in how it (i) administered a mandatory insurance program related to its auto loans, and (ii) charged certain borrowers for mortgage interest rate-lock extensions.
- Wells Fargo required to remediate harmed consumers and undertake activities related to its risk management and compliance management.
- CFPB assessed a $1 billion civil penalty but credited the $500 million penalty collected by the OCC toward satisfying its fine.
- CFPB posits that Wells engaged in such practices, which it could have avoided had it attended to certain information/reports as provided by its vendors.

Ballard Spahr LLP

Teachable Moments – Consent Orders

National Credit Adjusters, LLC/Hochstein Consent Order (July 13, 2018)

- NCA and Hochstein found in violation of UDAP and FDCPA for continuing to utilize and assisting their network of agencies and debt buyers to engage in unfair and deceptive acts and practices.
- Did so despite their own compliance personnel's recommending termination of such relationships due to multiple violations of law found as a result of NCA's vendor compliance program, and refused to implement corrective recommendations of such personnel.
- Actively assisted such agencies in appearing to be compliant to original creditors, and in persuading them to allow accounts to be placed with such agencies despite their violations of law.

Ballard Spahr LLP

Teachable Moments – FDIC FIL-19-2019

FDIC's FIL-19-2019 calls out perceived inadequacies in contractual treatment of rights and responsibilities regarding business continuity and incident response

- Reporting on deficiencies being found in the course of supervisory exams.
- Focus on technology service provider contracts
- Issues with inadequate business continuity plan requirements and business recovery plans
- Reminder of notification requirements under Section 7 of the Bank Service Company Act

Ballard Spahr LLP

Teachable Moments – Takeaways

- ✓Third party vendor risk management is still a "top of mind" issue for regulators
- ✓CFPB (and OCC, FDIC) remain very willing to pursue organizations for failures of third party oversight (including for failure to act upon information received), especially where they find resultant quantifiable consumer harm
- ✓This can get expensive!
- ✓Having a good program is not enough if you are not actively evolving

Ballard Spahr LLP

Ballard Spahr LLP

Questions?

Glen P. Trudel
Partner
302.252.4464
trudelg@ballardspahr.com

Ron K. Vaske
Partner
612.371.3215
vaskerk@ballardspahr.com

Judy M. Mok
Of Counsel
646.346.8008
mokj@ballardspahr.com

Ballard Spahr LLP

Ballard Spahr LLP

Cannabis, Artificial Intelligence, Machine Learning, Data Aggregation, Debt Collection, Prescreening and More: Regulatory Developments Affecting Card Issuers

Mark Furletti
Partner
215.864.8138
furlettim@ballardspahr.com

Ron Vaske
Partner
612.371.3215
vasker@ballardspahr.com

Stefanie Jackman
Partner
678.420.9490
jackmans@ballardspahr.com

Terence Grugan
Of Counsel
215.864.8320
grugant@ballardspahr.com

Ballard Spahr LLP

Ballard Spahr LLP

Machine Learning & Big Data

Ballard Spahr LLP

What is big data?

- Datasets whose size is beyond the ability of typical software tools to capture, store, manage and analyze (McKinsey)
- The 3 V's
  - Volume
  - Velocity
  - Variety

Ballard Spahr LLP

What is machine learning?

- Type of artificial intelligence
- Computer continuously figures out the best equation to solve a problem
- Computer has ability to "learn" without additional programming
- Can make relatively accurate predictions based on past observations

Ballard Spahr LLP

Uses of big data and machine learning

- Predictive policing
- Handwriting recognition
- Speech recognition
- Real estate pricing
- Spam filters
- Self-driving cars
- You might also like…
- Interpreting "wearables" data
- Hiring decision process
- And, of course, fraud and credit risk models

Ballard Spahr LLP

An oversimplified credit-related example

Potential ingredients for "default prediction stew"/input variables

- FICO
- Income
- Homeownership
- Number of delinquencies
- Amazon purchase history
- Facebook likes
- Color of primary vehicle
- Internal creditor data, including default data

Ballard Spahr LLP

An oversimplified example (cont'd)

Machine learning can answer these questions:

- Which ingredients will make the stew taste the best? i.e., which subset of these variables are most predictive of defaults?
- How much of each ingredient should we add? i.e., what weights should these variables be given in a model trying to predict defaults?
- How should we revise the recipe to account for changes in taste preferences or diner expectations? i.e., as time passes, how should these variables or their weights change?

The CFS attorney's challenge

- Ensuring that the machine-created stew does not run afoul of:
  - Anti-discrimination laws
  - Credit reporting laws
  - Data security laws
  - Privacy laws

Recent reports exploring regulatory issues

- Exec. Office of the President, Big Data: A Report on Algorithmic Systems, Opportunity and Civil Rights (May 2016)
- OCC, Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective (Mar. 2016)
- FTC, Big Data: A Tool for Inclusion or Exclusion? (Jan. 2016)
- CFSI, Big Data, Big Potential: Harnessing Data Technology for the Underserved Market (Mar. 2015)

Types of big data that pose challenges

- Social media connections/relationships
- Academic records/educational background
- Job type/status
- Online shopping purchase patterns/behaviors
- Website subscriptions
- GPS/location data
- IP address

Regulatory challenges

- Data accuracy
- Correlation vs. causation
- Fair lending
- NOAAs and RBP notices
- Securing data

Ballard Spahr LLP

Ways of addressing regulatory challenges

- High/medium/low risk classifications for variables
- Approval for any new variables
- Human review of all NOAA reasons
- Automated FL testing (using machine learning?)
- Complaint monitoring

Ballard Spahr LLP

Ballard Spahr LLP

Data Aggregation

Ballard Spahr LLP

Screen scraping vs. APIs

- Technical differences
- Pros & cons
- Trend towards bilateral API agreements
- Authentication & data security issues
  - Disclosing usernames and passwords
  - OAuth as a solution

Ballard Spahr LLP

Use Cases

- Consolidated account views
- Account and income validation
- Personal financial management tools
  - Budgeting
  - Optimized product usage & product selection
- Enhanced underwriting
- Artificial intelligence

Ballard Spahr LLP

Account Opening & Management

- Account opening & CIP
  - Instantaneous validation v. micro deposits
- Account consolidation
  - One dashboard for all accounts
  - Comprehensive portfolio snapshot
  - Total net worth (assets & liabilities)
- Potential Issues
  - Consumer consent, transparency
  - Limits & termination
  - Data security
  - Liability for unauthorized access

Ballard Spahr LLP

Higher-Value Features & Marketing

- Financial tools
  - Cash flow
  - Savings recommendations (automation & nudges)
  - Overdraft avoidance
  - Asset allocation, investment strategies, debt repayment strategies
- Optimized Product Recommendations & Marketing
  - Credit cards with better rates
  - Consolidate debt with personal loans
  - Refinance mortgage and student loans
- Potential Issues
  - Privacy
  - Providing financial advice
  - UDAAPs (e.g., accuracy & suitability)

Ballard Spahr LLP

Use of Data Aggregation in Making Eligibility Determinations

- Key issue is whether data aggregator is subject to FCRA
- Is the data aggregator providing "consumer reports"?
  - communication of information
  - by a CRA (circular)
  - bearing on an [identifiable] consumer's "seven factors"
  - which are used or expected to be used or collected
  - for the purpose of serving as a factor in establishing eligibility

Ballard Spahr LLP

Use of Data Aggregation in Making Eligibility Determinations (cont'd)

- Is the data aggregator a "consumer reporting agency"?
  - regularly engages in assembling or evaluating credit information
  - on consumers
  - for the purpose of providing reports to third parties
  - [and maintains "files"]

Principles for Safe Data Aggregation Activities

- CFPB's Principles on Data Aggregation
  - Access
  - Data Scope and Usability
  - Control and Informed Consent
  - Authorizing Payments
  - Security
  - Access Transparency
  - Accuracy
  - Ability to Dispute and Resolve Unauthorized Access
  - Efficient and Effective Accountability Mechanisms

Ballard Spahr LLP

Prescreening, Prequalifying, and Postscreening

Ballard Spahr LLP

Firm Offers

- "Any person who uses a consumer report on any consumer in connection with any credit or insurance transaction that is **not initiated by the consumer**, that is provided to that person under section 1681b(c)(1)(B) of this title, shall provide with each written solicitation made to the consumer regarding the transaction a clear and conspicuous statement that..."

FCRA § 615(d)

Ballard Spahr LLP

Firm Offers (cont'd)

- "The term "firm offer of credit or insurance" means any offer of credit or insurance to a consumer that **will be honored** if the consumer is determined, based on information in a consumer report on the consumer, to meet the specific criteria used to select the consumer for the offer, except that **the offer may be further conditioned on one or more of the following**:"

FCRA § 603(l)

Ballard Spahr LLP

Firm Offers (cont'd)

- "The consumer being determined, based on information in the consumer's application for the credit or insurance, to meet specific criteria **bearing on credit worthiness** or insurability, as applicable, that are **established**—

  (A) **before selection** of the consumer for the offer; and

  (B) for the purpose of determining whether to extend credit or insurance pursuant to the offer."

FCRA § 603(l)(1)

Ballard Spahr LLP

Firm Offers (cont'd)

- "Verification—

  (A) that the consumer continues to meet the specific criteria used to select the consumer for the offer, **by using** [1] information in a **consumer report** on the consumer, [2] information in the consumer's **application** for the credit or insurance, [3] or **other information** bearing on the credit worthiness or insurability of the consumer; or

  (B) of the **information in the consumer's application** for the credit or insurance, to determine that the consumer meets the specific criteria bearing on credit worthiness or insurability."

FCRA § 603(l)(2)

Ballard Spahr LLP

Prescreen vs. Prequalification

- Consumer experience
- Written consent requirement
- Permissible purpose
- Data returned – Full credit report vs. name/address
- Opt-outs eligible
- Inquiry type – soft/hard
- Prescreen disclosures
- Adverse action notices
- Firm offer

Ballard Spahr LLP

Ballard Spahr LLP

Recent FTC Actions

Ballard Spahr LLP

FTC Settles with Online Lending Company

- According to the FTC's complaint, the company:
  - Falsely advertised it would accept payments by debit or credit card, when it in fact rejected these forms of payment
  - Withdrew money from consumer accounts or charged credit cards without authorization

Ballard Spahr LLP

FTC Settles with Online Lending Company

- The Commission additionally charged law violations of:
  - Failing to properly and timely credit payments made by check
  - Providing inaccurate payoff quotes
  - Collecting additional amounts even after customers paid the quoted payoff amount
  - Requiring borrowers to agree to recurring automatic debits of their bank accounts as a condition of obtaining a loan

FTC Settles with Online Lending Company

- In addition to the monetary judgement, the company is prohibited from:
  - Taking unauthorized payments and from collecting payments via remotely created checks (RCC)
  - Misrepresenting accepted payment methods, the payoff amount, when payments will be applied/credited, or any material fact regarding payments, fees, or charges

FTC Settles with Online Lending Company

- The Commission vote approving the settlement was 5-0
- "Online lenders need to understand that loan servicing is just as important to consumers as loan marketing and origination, and we will not hesitate to hold lenders liable for unfair or deceptive servicing practices." –Andrew Smith, Director of the FTC's Bureau of Consumer Protection

Company Charged with Deceiving Consumers by FTC

- The FTC's complaint, approved by a vote of 2-0, alleges that the company misled consumers that their loans would not include "hidden fees" when in fact the company deducted hundreds or even thousands of dollars in hidden up-front fees from the loan.
- Additionally, the FTC alleges the company falsely told applicants that "Investors Have Backed Your Loan" knowing that many would never get a loan, which delayed applicants from seeking loans elsewhere

Company Charged with Deceiving Consumers by FTC

- Despite a warning from an attorney for one of the company's largest investors and an internal review which noted that the claims could be perceived as deceptive, the company engaged in the practice and made its deceptive "no hidden fees" claim even more prominent
- The company is charged with violating the FTC Act and the Gramm-Leach-Bliley Act

Ballard Spahr LLP

Ballard Spahr LLP

Prepaid Rule

Ballard Spahr LLP

Now In Effect: Prepaid Rule

- April 1 effective date, requirements include:
  - Pre-acquisition disclosures (short/long form, "close proximity," on-access device)
  - Compliance with new Reg. E requirements (periodic statements, error resolution, etc.)
  - Compliance with Reg. Z for hybrid prepaid-credit
  - Posting/submission of account agreements
- Scope analysis: if covered, look for exclusion

Ballard Spahr LLP

Prepaid Rule Compliance Challenges

- Consistency across all pre-acquisition disclosures (and other account materials)
- Highly specific requirements for short-form (e.g., $0 versus N/A); *cf.* flexible requirements with inadequate guidance for long-form (esp. variable fees)
- Preparing/testing forms for use in virtual environment
- IT/reporting capabilities for rolling 30-day window
- Fee types for pre-acquisition disclosures—concepts and calculations (e.g., 5% threshold for "other fee types")

Ballard Spahr LLP

Ballard Spahr LLP

Anti-Money Laundering

Ballard Spahr LLP

Background of BSA

- The current Anti-Money Laundering (AML)/Countering the Financing of Terrorism (CFT) regime is an amalgamation of statutes and regulations that generally derive from the Bank Secrecy Act (BSA), which was passed in 1970.
  - The purpose of the BSA, as stated in the statute, is to provide highly useful information to law enforcement.
  - The BSA generally requires financial institutions to maintain an AML program, know-their-customer (KYC), keep certain records and provide certain reports to the government, notably those on cash transactions over $10,000 (CTRs) and suspicious activity (SARs).
  - BSA requirements are further magnified by the wide-reaching and complex network of state and federal government actors – with different missions and incentives – who are responsible for implementing, enforcing and utilizing the information produced by the regime.

Ballard Spahr LLP

Current Issues

- Fraud Litigation
  - Fraud victims pursuing banks utilized by fraudsters
- Transaction Laundering
  - AKA Credit Card Laundering or Factoring
  - $200 Billion Per Year in elicit transactions
  - Enforcement Priority
- Cannabis Banking
  - Recent Legislation Easing Restrictions

Fraud Litigation

- Ponzi Schemes; Securities Fraud; Consumer Fraud
  - Fraudsters use bank accounts to receive funds from victims
  - Fraudsters maintain bank accounts for fraudulent enterprise
  - Fraudsters misappropriate victims funds from accounts
- Litigation against banks
  - Failure to detect
  - Failure to prevent
  - Aiding and abetting

Transaction Laundering

- Micro-transactions made through a merchant's payment credentials
- Processing credit card payments for unknown or illicit goods
- How does it work?
  - Criminal establishes shell company or website for legitimate-sounding business
  - Payments for illegal goods or actions channeled through shell merchant
- $200 billion problem

Ballard Spahr LLP

Cannabis Banking

- Marijuana remains Scheduled I controlled narcotic under federal Controlled Substances Act ("CSA"):
- Money laundering statutes: 18 U.S.C. §§ 1956 and 1957
- NYDFS published July 3, 2018 Guidance to "clarify the regulatory landscape and encourage" New York, state-chartered banks and credit unions to "offer banking services" to "marijuana related businesses licensed by New York state."
- Secure and Fair Enforcement Banking Act of 2019:
  - Introduced in House on March 7, 2019
- Prohibits a federal banking regulator from:
  - (1) terminating or limiting the deposit insurance or share insurance of a depository institution solely because institution provides financial services to a legitimate marijuana-related business; (2) prohibiting or otherwise discouraging a depository institution from offering financial services to such a business; (3) recommending, incentivizing, or encouraging a depository institution not to offer financial services to an account holder solely because the account holder is affiliated with such a business; or (4) taking any adverse or corrective supervisory action on a loan made to a person solely because the person either owns such a business or owns real estate or equipment leased or sold to such a business.
- Removed liability/forfeiture exposure for depository institution providing loan or other financial services to legitimate marijuana-related business.

Ballard Spahr LLP

Ballard Spahr LLP

Debt Collection

Ballard Spahr LLP

The CFPB's Collections NPRM

- Released on May 8, 2019
- This is a third-party rule, right? *Yes.*
- So why are we talking about it?
  - CFPB Bulletin 2013-07 and UDAAP
  - State laws and regulations
  - Vendor oversight responsibilities
  - Obligations that will have a direct impact on **you**

Ballard Spahr LLP

The NPRM and You

- Using non-work phone numbers and emails to contact consumers:
  - Broad initial contractual consent & proof of last use of email/phone number (§ 1006.6(d)(3))
  - Valid E-SIGN consent (§ 1006.42(b) – (d))
  - Opt-out/C&D request tracking (§ 1006.6(e))
- Time/place/manner restrictions
  - Unusual time/place (§ 1006.6(b))
  - Call limitations (§ 1006.14(b))
    - Attempted communication – limited to 7 attempts in 7 days per account*; limited content messages included
    - Communication (included leaving a voice message) – 7 days waiting period

The NPRM and You

- Limited content messages are not collection communications (§ 1006.2(b), (d), (j))
  - Communication = the conveying of information regarding a debt directly or indirectly to any person through any medium. . . " (§ 1006.2(d)
  - Attempt to communicate = "any act to initiate a communication or other contact with any person through any medium, including by soliciting a response (§ 1006.2(b)
  - No company name in the message, which prohibits email
- Time-barred debt (§ 1006.26)

The NPRM and You

- Definition of "debt collector" and *Henson v. Santander* (§1006.2(i)
  - Principal purpose prong OR
  - Regularly collects/attempt to collect debts
- Debt sales (§ 1006.30(b)) – prohibit if:
  - Discharged in bankruptcy
  - Paid/settled
  - Identity theft report "has been filed"
- Additional provisions:
  - Debt validation, decedent debt, credit reporting restrictions, LEP disclosures, no work email generally, no social media except through private messaging function

Ballard Spahr LLP

Ballard Spahr LLP

Questions?

Mark Furletti
Partner
215.864.8138
furlettim@ballardspahr.com

Ron Vaske
Partner
612.371.3215
vasker@ballardspahr.com

Stefanie Jackman
Partner
678.420.9490
jackmans@ballardspahr.com

Terence Grugan
Of Counsel
215.864.8320
grugant@ballardspahr.com

Ballard Spahr LLP

Ballard Spahr LLP

Trends in Consumer Litigation

Stefanie Jackman
Partner
678.420.9490
jackmans@ballardspahr.com

Daniel McKenna
Partner
215.864.8321
mckennad@ballardspahr.com

Ballard Spahr LLP

The Big Three

FDCPA, FCRA, TCPA, Oh My

	Current Month:	Previous Month:		Previous Year:		Year to Date:	Year to Date Comp:	
	Mar 01, 2019 Mar 31, 2019	*Feb 01, 2019 Feb 28, 2019*		*Mar 01, 2018 Mar 31, 2018*		*Jan 01, 2019 Mar 31, 2019*	*Jan 01, 2018 Mar 31, 2018*	
CFPB	4133	3834	7.8%	5308	-22.1%	11136	14838	-24.9%
FDCPA	722	660	9.4%	844	-14.5%	2099	2447	-14.2%
FCRA	350	386	-9.3%	372	-5.9%	1085	1102	-1.5%
TCPA	287	266	7.9%	343	-16.3%	855	955	-10.5%

Webrecon.com

Ballard Spahr LLP

"Send him our toughest collection letter, threaten him with legal action, and subliminally suggest some type of bodily harm. But put XOXOXO under my signature to show that we still love him as a customer!"

FDCPA Statistics

- Consistently most filed lawsuit in the country
- Filings down 24.9% from 2018, but volume is on the rise
- 18.4% filed as class actions
- Top three issues
  - 48% debt not owed
  - 21% errors in notification
  - 13% communication tactics

Why Do I Care About The FDCPA

- CFPB Bulletin 2013-07 – applies portions of the FDCPA to first-party creditors through UDAAP
  - May 8, 2019 NPRM – a number of proposed prohibitions implemented through UDAAP
  - Collections-related exams and enforcement continue
- State laws and licensing regulations that adopt the FDCPA and apply it more broadly
  - FDCPA can impact interpretation and application of those statutes
- State private litigation risk

Ballard Spahr LLP

FDCPA Litigation Trends

- Identifying the caller and creditor
- Validation notice
  - First-party applications in MA, NYC (accelerated debt only), and CA
- Unauthorized third-party disclosures of the debt
- Debt itemization
- 1099C disclosures
- Time-barred debt disclosures
- Documentation, documentation, documentation

Ballard Spahr LLP

Ballard Spahr LLP

FCRA Statistics

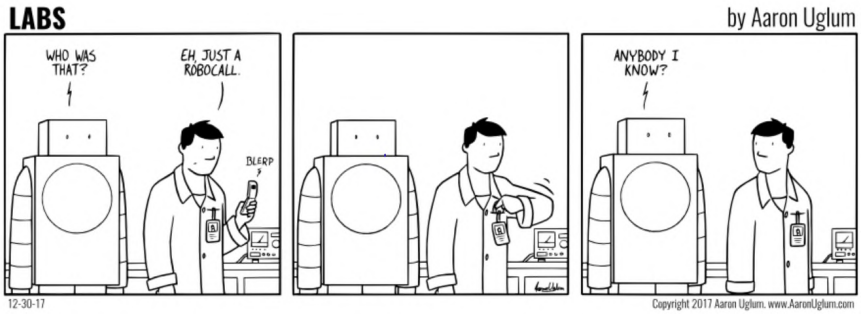
- Number of filings increased every year since 2011
- 2nd most filed case in 2018 (4,531)
- 2nd most filed case in 2019 YTD
- 2019 filings are down 1.5% YTD, but only because of slow March
- Average of 8% are brought as class actions

Ballard Spahr LLP

FCRA Trends

- Statute of limitations
  - *Escobar v. Pa. Higher Educ Assistance*, 2018 U.S. Dist. LEXIS 61004 (E.D. Pa. April 11, 2018)
- Technical accuracy versus misleading impression
  - *Schweitzer v. Equifax Info. Sol., LLC*, 441 F. App'x 896 (3d Cir. 2011)
- Challenges to legal determinations
  - *Denan v. TransUnion*, 2019 U.S. Dist. LEXIS 30694 (N.D Ill. Feb. 22, 2019) (FCRA cannot be used to challenge legal determinations)
- Impermissible Purpose
- Bankruptcy Designations

Ballard Spahr LLP



Ballard Spahr LLP

TCPA Statistics

- Demoted to third most filed lawsuit in 2018
- 10.5% fewer filings compared to 2018
- But ...
  - 41.8% of filings are class actions
  - Large number of pre-lits and arbitration demands
  - Remains the number 1 complaint to FCC and FTC

Ballard Spahr LLP

TCPA Trends

- ATDS
  - Number Generation
    - Dominguez v. Yahoo, Inc.
    - King v. Time Warner
    - Marks v. Crunch
  - Human Intervention
    - *Kolkerts v. Seterus, Inc.*, No. 17-cv-4171, 2019 U.S. Dist. Lexis 42347 (N.D. Ill. Mar 15, 2019)
  - FCC Guidance

Ballard Spahr LLP

TCPA Trends

- Text Messaging
  - *Viggiano v. Kohls*, No. 17-cv-00243 (D.N.J. 2017)
  - *Duran v LaBoom Disco,* No. 17-cv-7331, 2019 U.S. Dist. LEXIS 30012 (E.D.N.Y.)
- Class Actions
  - *West v. California Services Bureau, Inc.,* 2017 WL 6316823 (N.D. Cal., 2017)
  - *Joanne Knapper v. Cox Communications Inc.,* Case No. 2:17-cv-00913 (D. Ariz. 2018)
  - *Tomeo v. CitiGroup, Inc.,* 2018 U.S.Dist.LEXIS 166117 (N.D. Ill. 2018)

TCPA Trends

- Reassigned number database
  - Database will include number and the date "the provider permanently has reversed its assignment of the number to the subscriber such that the number has been disassociated with the subscriber."
  - Must supply the number being queried and "either the date they contacted the customer or the date on which the caller could be confident that the consumer could still be reached at that number."
- TRACED Act
- Manufactured Litigation
  - *Shelton v. Target Advance LLC,* 2019 U.S. Dist. LEXIS 64713 (E.D. Pa April 16, 2019) and *D'Ottavio v. Slack Techs*., 2019 U.S. Dist. LEXIS 64069 (D. N.J. April 15, 2019)

Ballard Spahr LLP

Questions?

Stefanie Jackman
Partner
678.420.9490
jackmans@ballardspahr.com

Daniel McKenna
Partner
215.864.8321
mckennad@ballardspahr.com

Ballard Spahr LLP

Ballard Spahr LLP

Privacy and Data Security:

Identifying Vulnerabilities and Emerging Threats

Kim Phan
Partner
202.661.7647
phank@ballardspahr.com

Ballard Spahr LLP

The Numbers

Financial and Insurance

Denial of Service and use of stolen credentials on banking applications remain common. Compromised email accounts become evident once those attacked are filtered. ATM Skimming continues to decline.

Frequency	927 incidents, 207 with confirmed data disclosure
Top 3 patterns	Web Applications, Privilege Misuse, and Miscellaneous Errors represent 72% of breaches
Threat actors	External (72%), Internal (36%), Multiple parties (10%), Partner (2%) (breaches)
Actor motives	Financial (88%), Espionage (10%) (breaches)
Data compromised	Personal (43%), Credentials (38%), Internal (38%) (breaches)

Verizon 2019 Data Breach Investigations Report

It's not easy ... do you recognize this?

6.4 billion The number of fake emails sent worldwide – every day[1]	**1,464** The number of government officials in one state using "Password123" as their password[2]
50% The number of local authorities in England relying on unsupported server software[3]	**2 million** The number of stolen identities used to make fake comments during a US inquiry into net neutrality[4]
1,946,181,599 The total number of records containing personal and other sensitive data compromised between January 2017 and March 2018[5]	**US$729,000** The amount lost by a businessman in a scam combining "catphishing" and "whaling"[6]
550 million The number of phishing emails sent out by a single campaign during the first quarter of 2018[7]	**US$3.62m** The average cost of a data breach last year[8]

EY Global Information Security Survey 2018-2019

The increase in the annual cost of cybercrime

$11.7m Average cost of cybercrime in 2017 → **$13.0m** Average cost of cybercrime in 2018 **+12%** Increase in the last year

Ponemon-Accenture 2019 Cost of Cybercrime Study

Ballard Spahr LLP

FTC Guidance

Cyber Criminals Target Companies of All Sizes

Knowing some cybersecurity basics and putting them in practice will help you protect your business and reduce the risk of a cyber attack.

Protect Your Files & Devices

Update your software
This includes your apps, web browsers, and operating systems. Set updates to happen automatically.

Secure your files
Back up important files offline, on an external hard drive, or in the cloud. Make sure you store your paper files securely, too.

Require passwords
Use passwords for all laptops, tablets, and smartphones. Don't leave these devices unattended in public places.

Encrypt devices
Encrypt devices and other media that contain sensitive personal information. This includes laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage solutions.

Use multi-factor authentication
Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.

Ballard Spahr LLP

FTC Guidance

Protect Your Wireless Network

Secure your router

Change the default name and password, turn off remote management, and log out as the administrator once the router is set up.

Use at least WPA2 encryption

Make sure your router offers WPA2 or WPA3 encryption, and that it's turned on. Encryption protects information sent over your network so it can't be read by outsiders.

Make Smart Security your Business as Usual

Require strong passwords

A strong password is at least 12 characters that are a mix of numbers, symbols, and capital and lowercase letters.

Never reuse passwords and don't share them on the phone, in texts, or by email.

Limit the number of unsuccessful log-in attempts to limit password-guessing attacks.

Train all staff

Create a culture of security by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. If employees don't attend, consider blocking their access to the network.

Have a plan

Have a plan for saving data, running the business, and notifying customers if you experience a breach. The FTC's *Data Breach Response: A Guide for Business* gives steps you can take.

Ballard Spahr LLP

Ballard Spahr LLP

California Consumer Protection Act

Ballard Spahr LLP

Key Dates

- **June 28, 2018**: CCPA signed into law.
- **Fall 2019**: CCPA implementing regulations to be issued by the California Attorney General.
- **January 1, 2020**: CCPA effective date.
- **Earlier of July 1, 2020 or 6 months after the implementing regulations are issued**: CCPA enforcement date.

CCPA Requirements

- Enhanced disclosures, including in online privacy policies and when personal information is collected.
- Consumer rights, including information access, the right to be forgotten, the right to opt out of certain third party information sharing, and the right to equal service regardless of exercising any privacy rights.
- Reasonable security procedures and practices appropriate to the nature of the information.
- Violations of these requirements could result in:
  - Civil penalties in the amount of $7,500 for each intentional violation and $2,500 for each unintentional violation; and
  - If the violation involves a data breach, a private right of action conferring statutory penalties between $100 to $750 per California resident and incident, or actual damages, whichever is greater.

Next Steps

- Resource allocation
- Data mapping
- Updating policies and procedures
- Review and revise vendor contracts

Ballard Spahr LLP

Ballard Spahr LLP

Gramm-Leach-Bliley Act

Safeguard Rule Amendments

Privacy Rule Amendments

Ballard Spahr LLP

Safeguards Rule Key Dates

- **March 5, 2019**: FTC announced updates.
- **April 4, 2019**: Notice of proposed rulemaking published in the Federal Register.
- **June 3, 2019**: Deadline to submit public comments on proposed changes.

Ballard Spahr LLP

New Safeguards Requirements

- Comprehensive written information security program must now include:
  - A written incident response plan
  - A chief information security officer (CISO) who will report annually to the Board
  - Access controls for authorized users
  - Encryption for personal information in transit and at rest
  - Secure development practices for internal applications
  - Multi-factor authentication for access to personal information, including employees and customers
  - Risk assessments
  - Audit trails to assist in detecting security events
  - Secure disposal procedures for personal information
  - Continuous monitoring or annual penetration testing and biannual vulnerability assessments
  - Enhanced service provider oversight
- Other administrative, technical, and physical safeguards that are appropriate to the size and complexity of the financial institution, the nature of its activities, and the sensitivity of any customer personal information; and that are reasonably designed to protect against threats and protect against unauthorized access.

Ballard Spahr LLP

Public Comment Opportunities

- Whether the small business exemption (entities with less than 5,000 customers) is too low.
- Whether compliance with other data security standards, such as the NIST Cybersecurity Framework and PCI-DSS should confer a safe harbor under the Safeguard Rule.
- Whether the granular approach being taken creates any unintended consequences for business.
- Whether the new requirements are more stringent that necessary to achieve the objective of improving data security in the industry.
- Whether the FTC should require notice of data breaches, and if so, (1) a reporting deadline, (2) risk of harm trigger, and (3) whether the FTC should make such reports public.
- Etc.

PayPal Consent Order

- On May 24, 2018, the FTC finalized a settlement against PayPal for violations of the GLBA Safeguards Rule by its peer-to-peer payment service, Venmo.
- The FTC alleged that Venmo failed to have a written information security program.
- The FTC also alleged that Venmo failed to implement basic safeguards to protect the security, confidentiality, and integrity of consumer information, including:
  - 1) Failing to provide security notifications to consumers, such as notifications that a consumer's password or e-mail address has changed, or that a new device was added to the consumer's account; and
  - 2) Failing to maintain adequate customer support to timely investigate and respond to users' reports concerning account compromise or unauthorized transactions.

Privacy Rule

- On August 10, 2018, the Consumer Financial Protection Bureau (CFPB) amended the GLBA Privacy Rule.
- The updates reflect statutory amendments as part of the FAST Act (2015). Financial institutions are no longer required to deliver an annual privacy notice under GLBA if:
  - There is no sharing of customer information that would trigger a customer opt out right, and
  - No changes have been made to the privacy notice since the one previously delivered to a customer.

Ballard Spahr LLP

Ballard Spahr LLP

Other Financial Regulatory Developments

Ballard Spahr LLP

FTC Red Flags Rule & Card Issuers Rule

- The Red Flags Rule requires financial institutions and some creditors to implement a written identity theft prevention program designed to detect the "red flags" of identity theft in their day-to-day operations, take steps to prevent it, and mitigate its damage.
- The Card Issuers Rule requires that debit or credit card issuers implement policies and procedures to assess the validity of a change of address request if, within a short period of time after receiving the request, the issuer receives a request for an additional or replacement card for the same account. Card issuers cannot issue an additional or replacement card until it has notified the cardholder about the request or otherwise assessed the validity of the address change.
- The Federal Trade Commission (FTC) is reviewing the rules for modification. The public comment period closed on February 11, 2019.

SEC Regulation S-ID

- For those financial institutions not subject to the FTC's jurisdiction, the Securities and Exchange Commission (SEC) has issues Regulation S-ID, which contains the same Red Flags Rule requirements.
- The SEC's first enforcement action under Regulation S-ID was announced on September 26, 2018 against Voya Financial Advisors.
  - In this case, "vishing" intrusion (voice phishing) allowed one or more persons impersonating Voya representatives to gain access to personal identifying information of approximately 5,600 customers.
  - $1 million civil penalty

SEC Cybersecurity Activity

- Yahoo breach (April 2018)
  - First enforcement action brought against a company for failure to publicly disclose a breach.
  - $35 million civil penalty.
  - $250 million reduction in Verizon purchase price.
- New Interpretive Guidance on Public Company Cybersecurity Disclosures (February 2018)
  - Public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion.
  - Directors, officers, and other corporate insiders must not trade a public company's securities while in possession of material nonpublic information, which may include knowledge regarding a significant cybersecurity incident experienced by the company.

Federal Financial Institutions Examination Council

- FFIEC Statement on OFAC Cyber-Related Sanctions (November 2018)
- Cybersecurity Resource Guide for Financial Institutions (October 2018)
- FFIEC Joint Statement on Cyber Insurance and Its Potential Role in Risk Management Programs (April 2018)
- Department of Justice Best Practices for Victim Response and Reporting of Cyber Incidents (September 2018)

NIST Privacy Framework

- "Good cybersecurity doesn't solve it all."
- In September 2018, the National Institute of Standards and Technology (NIST) announced a collaborative project to develop a "voluntary" Privacy Framework. The goal is to establish an enterprise risk management tool to help organizations prioritize strategies for flexible and effective privacy protection solutions so that individuals can enjoy the benefits of innovative technologies.
- The public comment period closed on January 14, 2019.
- The first discussion draft was released on April 30, 2019.
- The second drafting workshop will be held on May 13-14, 2019 in Atlanta, GA.

Ballard Spahr LLP

Ballard Spahr LLP

Questions?

Kim Phan
Partner
202.661.7647
phank@ballardspahr.com

Ballard Spahr LLP