FINANCIAL SERVICES REPORT

Quarterly News, Winter 2016

Award Winning Newsletter

IN THIS ISSUE

MOFO METRICS

20	Number of cards and packages delivered by the U.S. Postal Service during the holiday season, in billions
4	Amount of trash from wrapping paper and shopping bags, in million tons
28	Number of LEGO sets sold during the holiday season, per second
17	Percentage of annual retail sales made during the holiday season
133.7	Number of consumers that shop in stores or online on Black Friday, in millions
403.35	Average amount spent on Black Friday, per person

Attorney Advertising

MORRISON FOERSTER

EDITOR'S NOTE

Hope you survived all of those awkward Thanksgiving holiday conversations—amazing how divided people are on whether the court got it right in the *PHH* case, isn't it? So on we go into the holiday season, while visions of Dodd-Frank repeal dance in our heads. No long winter's nap for the CFPB, not with the inauguration fast approaching. Will we see a final arbitration rule in our stockings? Will the New Year bring efforts to reinstate Glass-Steagall? How about the promised temporary moratorium on new agency regulations?

No crystal ball, but read on to learn the latest in privacy, mortgage, arbitration, etc., etc. The *PHH* ruling, the Financial Choice Act, the OCC's take on regulating FinTech, the latest on privacy, preemption, arbitration, and mortgage—it's all here as our present to you.

Until next time, have a wonderful holiday and a Happy New Year, from all of us to all of you.

BELTWAY

Don't Mess with Servicemembers

In September 2016, the OCC entered into a consent order with a national bank, alleging that the bank violated the Servicemembers Civil Relief Act (SCRA). The OCC asserted that the bank failed to (1) reduce the interest rate charged on loans to 6%, (2) obtain court orders before repossessing servicemembers' automobiles, and (3) accurately describe servicemembers' military status in certain affidavits filed in eviction proceedings. The OCC assessed a $20 million civil money penalty in connection with the order.

For more information, contact Leonard Chanin at lchanin@mofo.com.

Federal Reserve: Don't Hide the Money

In September 2016, the FRB (the "Board") entered into an order with the Agricultural Bank of China, including the New York branch of the Agricultural Bank of China. The Board found significant deficiencies in the bank's risk management practices and in its compliance with AML and BSA provisions. Under the order, the bank must provide a written plan to enhance oversight of compliance with AML/BSA requirements.

For more information, contact Barbara Mendelson at bmendelson@mofo.com.

FTC Drives Away a Winner

In October 2016, the FTC announced that a federal district court had approved an award of $1.3 billion from Scott Tucker and companies owned by Mr. Tucker, including AMG Capital Management (AMG) for engaging in allegedly deceptive and other unlawful practices in connection with making payday loans and collecting on those loans. The ruling follows several years of actions by the FTC against Mr. Tucker and his companies. Mr. Tucker had asserted that the FTC lacked jurisdiction because the loans were made by AMG, which is affiliated with Native American tribes with sovereign status.

For more information, contact James McGuire at jmcguire@mofo.com.

Nothing Foreign About OCC Risk Management Guidance

In October 2016, the OCC issued risk management guidance, noting that banks should conduct periodic risk re-evaluations for portfolios that contain foreign correspondent accounts. The guidance addresses "best practices" that banks should consider when conducting periodic re-evaluations of risks related to such accounts, including establishing and maintaining an effective governance function for those accounts. The guidance includes a discussion about banks' decisions whether to retain or terminate such accounts.

For more information, contact Oliver Ireland at oireland@mofo.com.

Surcharges in the Spotlight at the Supreme Court

In September 2016, the U.S. Supreme Court agreed to hear the Second Circuit case of *Expressions Hair Design v. Schneiderman*. The issue presented is whether state laws that prohibit "surcharges" on credit cards unconstitutionally restrict speech about price information (as the Eleventh Circuit holds) or whether such laws regulate economic conduct (as the Second and Fifth Circuits hold). State "no-surcharge" laws allow merchants to charge higher prices to consumers who pay with a credit card (instead of cash) and allow merchants to describe the difference as a cash "discount," but not as a "surcharge."

For more information, contact Michael Miller at mbmiller@mofo.com.

BUREAU

CFPB Finalizes Sweeping Prepaid-Account Rule

The Bureau issued its final comprehensive (1,700-page) new rule regulating prepaid accounts in October. The rule defines prepaid accounts and provides examples of the types of accounts that qualify. The rule requires financial institutions to limit consumers' losses when funds are stolen or cards are lost; investigate and resolve errors; and provide consumers with free and accessible account information. It adopts Regulation E's dispute resolution framework, declining to accept industry comments advocating greater flexibility depending on the type of prepaid account. The rule also establishes Know Before You Owe disclosure requirements and comprehensive consumer protections, including requirements related to credit features available in connection with a prepaid card (so-called "hybrid prepaid-credit cards"). The rule will take effect on October 1, 2017, with exceptions for issuers that lack sufficient data to provide account history and disclosure requirements for cards manufactured prior to October 1, 2017.

For more information, read our Client Alert or contact Obrea Poindexter at opoindexter@mofo.com.

More Flexibility for Service Providers

The Bureau is adjusting its approach to service providers, reissuing guidance to provide additional flexibility to implement risk management programs. The guidance clarifies that "the depth and formality of the risk management program for service providers may vary

depending upon the service being performed," namely, by "its size, scope, complexity, importance and potential for consumer harm." The Bureau noted that it expects that supervised banks will monitor their relationships with service providers to ensure compliance with applicable consumer financial laws, and emphasizes that due diligence by supervised banks or other entities—while not "a shield against liability"—can reduce the risk of liability.

For more information, contact Nancy Thomas at nthomas@mofo.com.

TILA Title Trouble

In September, the CFPB sued five Arizona title lenders for allegedly failing to disclose their APR's in online advertisements, in violation of TILA. The CFPB alleged that the companies advertised a periodic interest rate for loans without listing the corresponding annual percentage rate. It acknowledged that one lender instructed consumers to take its advertised rate and multiply it by 12, but said that the lender failed to disclose that this calculated number would be the APR.

For more information, contact David Fioccola at dfioccola@mofo.com.

CFPB Stays on the Auto Finance Bandwagon

An auto title lender will pay a $9 million penalty in connection with a CFPB Consent Order for allegedly abusive loan-repayment practices. The CFPB alleged that the lender encouraged consumers to repeatedly renew their loans, without disclosing the full cost of doing so. The company's employees were also alleged to have visited consumers' homes, references, or places of employment to collect debts, illegally exposing information about these consumers' debt.

For more information, contact Jessica Kaufman at jkaufman@mofo.com.

Online Consumer Lending Stays in the Hot Seat

The CFPB entered into a Consent Order with an online lender in September, alleging unfair and deceptive practices related to marketing and advertising, fees, and consumer reporting. According to the CFPB, the lender failed to deliver benefits that it advertised or to disclose certain fees associated with its products. As part of the Consent Order, the lender paid over $3 million in restitution and civil monetary penalties. It also simultaneously entered into a settlement agreement with the California DBO related to California payday and installment lending laws.

For more information, contact James McGuire at jmcguire@mofo.com.

OIG to CFPB: Get Serious About Info Security

The Office of the Inspector General issued a report criticizing the CPFB's information security. The report acknowledged that the CFPB had taken some steps to develop and implement an information-security continuous monitoring program consistent with federal requirements. It highlights, however, several weaknesses, including a lack of processes to detect and protect against unauthorized access to and disclosure of sensitive information; overreliance on third-party contractors to provide cloud-based services; a lack of employee awareness of and compliance with existing policies and procedures; and gaps in financial reporting related to property, equipment, and software.

For more information, contact Nate Taylor at ntaylor@mofo.com.

More MLA Exam Procedures

The Bureau issued updated procedures for examining lenders for compliance with the Military Lending Act (MLA) rules that the Department of Defense issued in July 2015. The MLA establishes protections for servicemember consumers, such as a 36% rate cap and prohibitions on mandatory arbitration, mandatory allotments, and other waivers of consumer protection laws. The new CFPB procedures, modeled on FFIEC procedures, will focus on financial institutions' compliance-management systems and overall efforts to follow the MLA rules' requirements. Examiners are directed to consider an institution's implementation plan, including actions taken to update policies, procedures, and processes, and its training of appropriate staff. The final procedures also include an examination flowchart and checklist.

For more information, contact Leonard Chanin at lchanin@mofo.com.

MOBILE & EMERGING PAYMENTS

Digital Wallets Meet New Reality

After more than two years in the incubator, the CFPB finalized its Prepaid Accounts Rule on October 5, 2016. The scope of the final rule is sweeping and includes digital wallets that are capable of storing funds and making purchases or P2P transfers. Digital wallets that only store payment credentials are not subject to the final rule. Many traditional prepaid card issuers have long provided a number of the disclosures and other consumer protections, but one of the main industries that will need to make fundamental changes are certain operators of digital wallets. Entities that operate digital wallets within the scope of the final rule are now required, along with

traditional prepaid issuers and program managers, to comply with all the consumer protection and disclosure requirements found in the final rule.

For more information, contact Obrea Poindexter at opoindexter@mofo.com.

Security v. Consumer Choice

In remarks at a Salt Lake Cityfield hearing on November 17, 2016, CFPB Director Richard Cordray came down squarely on the side of empowering consumers to access their financial records through the use of so-called data aggregators. Data aggregators collect consumer information from financial institutions and typically make that information available to app and web developers for services used by the consumer, such as personal financial management websites and apps. Following the field hearing, the CFPB published a Request for Information (RFI) regarding data aggregation services and access to consumer financial information. With its RFI, the CFPB is attempting to mediate between FinTech companies developing new services to consumers using consumer data, and traditional financial institutions worried about the privacy and data security aspects of using that data. Comments for the RFI will be due 90 days after its publication in the *Federal Register*.

For more information, contact Trevor Salter at tsalter@mofo.com.

Regulatory Sandbox for Blockchain? Don't Grab Your Shovels Yet

During a speech at the Institute on International Finance, Federal Reserve Governor Lael Brainard quashed calls for a regulatory sandbox and widespread implementation of blockchain in the financial services industry by asserting that the technology is still in its developmental stage. FinTech advocates have pointed to the tangible benefits that blockchain has to offer, such as real-time payment settlement, and complained that the U.S. is lagging dangerously behind more innovative countries such as the United Kingdom, where regulators do permit an experimentation sandbox. But Governor Brainard reminded her audience that, for the moment, significant security concerns remain, including the open, distributed nature of the blockchain and a lack of common protocols and best practices for dealing with a breach on the blockchain. Brainard also noted that the financial services industry remains concerned with end-point security, exacerbated by recent Bitcoin hacks involving the theft of cryptographic keys. Yet Brainard remained optimistic about the future, "recognizing this may represent the most significant development in many years in payments, clearing, and settlement."

For more information, contact Jeremy Mandell at jmandell@mofo.com.

OCC Wades Deeper Into FinTech

On October 26, 2016, the OCC released its Recommendations and Decisions for Implementing a Responsible Innovation Framework, which helps pave the way for increased innovation and adoption of FinTech. Although the framework does not discuss the oft-rumored federal FinTech charter, it does implement a number of important recommendations. The framework establishes a standalone Office of Innovation within the OCC, which will serve as a central point of contact, conduct outreach, enhance awareness and education, monitor the evolving industry landscape, and collaborate with other regulators. The office will be led by the newly appointed OCC Chief Innovation Officer, Beth Knickerbocker, and will share many similarities with the CFPB's Project Catalyst. To foster innovation and outreach, the office will hold "office hours," workshops, and roundtables to facilitate discussion on industry-specific topics. One of the other key duties of the office will be to provide technical assistance to banks and nonbanks, including FinTech providers. Although the framework does mention the development of an optional bank-run pilot program, Comptroller of the Currency Thomas Curry has expressly ruled out any sort of "safe space" or regulatory sandbox for FinTech companies.

For more information, contact Sean Ruff at sruff@mofo.com.

MORTGAGE & FAIR LENDING

CFPB Hit by Major Setback; Asks for Review

In a decision eagerly awaited by the financial services industry, the D.C. Circuit handed the CFPB a major defeat, throwing out a mortgage lender's $109 million disgorgement remedy on multiple independent grounds. *PHH Corp. v. CFPB*, 839 F.3d 1 (D.C. Cir. 2016). First, the court held that the CFPB's structure is unconstitutional. Second, it rejected the CFPB's reading of RESPA, holding that RESPA Section 8(c) is a real safe harbor that "allows captive reinsurance arrangements so long as the amount paid by the mortgage insurer for the reinsurance does not exceed the reasonable market value of the reinsurance." Third, it ruled that the disgorgement remedy imposed on PHH violated fair-notice principles rooted in the Due Process Clause and administrative law. And finally, it rejected the CFPB's position that no statute of limitations applied to the administrative enforcement proceedings, holding instead that a three-year limit applies. This isn't the end of the story, though. The CFPB petitioned the D.C.

Circuit for *en banc* review, describing the decision as "what may be the most important separation-of-powers case in a generation."

For more information, read our Client Alert or contact Don Lampe at dlampe@mofo.com.

Ninth Circuit Deepens FDCPA Split

The Ninth Circuit has deepened the circuit split on whether the FDCPA applies to mortgage foreclosures. *Ho v. ReconTrust Co.*, 840 F.3d 618 (9th Cir. 2016). The Fifth and Eleventh Circuits, and various district courts, have held that the enforcement of a security interest doesn't meet the FDCPA's definition of "debt," and thus the statute doesn't normally apply to foreclosures. Courts in the Third, Fourth, and Sixth Circuits have taken the opposite position. The Ninth Circuit has now joined the Fifth and Eleventh Circuits, holding that foreclosures are not "debt" under the FDCPA. The court held that the trustee handling the foreclosure was not subject to the FDCPA because it is not a "debt collector." In doing so, the Ninth Circuit rejected the CFPB's *amicus* arguments.

For more information, contact Angela Kleine at akleine@mofo.com.

CFPB: ECOA Protects LGBT Borrowers

The CFPB issued a letter stating that ECOA and Regulation B prohibit credit discrimination on the basis of gender identity or sexual orientation. Responding to an inquiry from an advocacy group, the letter concludes that the statute's protections against discrimination on the basis of sex should be read to cover discrimination based on gender identity and sexual orientation, including discrimination based on "actual or perceived nonconformity" with gender-based stereotypes.

For more information, read our Client Alert or contact Leonard Chanin at lchanin@mofo.com.

HMDA or the Highway

In October, the CFPB blitzed 44 mortgage lenders and brokers with letters warning that they may be failing to comply with HMDA data-reporting requirements. The Bureau strongly "encouraged" recipients to "respond to the Bureau to advise if they have taken, or will take, steps to ensure compliance with [HMDA]," or "tell the Bureau if they think the law does not apply to them." In its news release, the CFPB emphasized its view that "[f]inancial institutions that fail to report mortgage information as required make it harder to identify and address discriminatory lending."

For more information, contact Angela Kleine at akleine@mofo.com.

HUD'S LEP Forward

On September 15, HUD issued guidance on how the FHA's nondiscrimination provisions apply to persons with Limited English Proficiency (LEP) in housing transactions. The guidance addresses liability for both intentional discrimination and practices that have a disparate impact on LEP individuals. While its primary focus is on rental discrimination, the guidance also discusses mortgage loan transactions, and alludes to the failure of housing providers to provide translation services. While HUD does not suggest that lenders must, or even should, provide such translation services, this is an important issue that will likely garner greater attention in the future.

For more information, read our Client Alert or contact Leonard Chanin at lchanin@mofo.com.

OPERATIONS

Stressed Out

This September, the OCC published guidelines establishing standards for recovery planning by certain regulated banks—those with average total consolidated assets of at least $50 billion. The guidelines address recovery planning for severe-stress events, including cyberattacks and other crises. They also provide a comprehensive framework for evaluating the financial effects of severe-stress events and the options for the covered bank to remain viable. OCC examiners will use the guidelines to assess the appropriateness and adequacy of a covered bank's recovery planning as part of regular supervisory activities. The OCC will phase in the guidelines over 18 months from January 1, 2017, depending on the size of the covered bank.

For more information, contact Oliver Ireland at oireland@mofo.com.

Foreign Funny Business

On October 5, 2016, the OCC issued guidance to regulated banks about periodic evaluations of the risks associated with foreign correspondent banking accounts. The guidance suggests particular anti-money laundering risks presented by foreign correspondent relationships that may result from a lack transparency to foreign bank clients that initiate transactions. It restates the OCC's expectation that regulated banks regularly reassess these risks. And it shares best practices to follow when making account retention and termination decisions, including establishing appropriate governance functions; communicating with foreign financial institutions before terminating their accounts, where appropriate; considering whether account closures will have an adverse impact on access to financial services for an entire group of customers or potential customers, or an entire geographic location; and making

termination decisions following a careful risk assessment of each individual foreign financial institution, as appropriate.

For more information, contact Barbara Mendelson at bmendelson@mofo.com.

Faster-Payments Proposals Under Review

The Federal Reserve Faster Payments task forces have started their review of 19 proposals for a faster payment system. The detailed proposals and preliminary assessments by McKinsey have been distributed to task force members, who include representatives from banks, consumer groups, payment service providers, financial technology firms, and government agencies. Following the review, the task forces will issue a two-part report. The first section of the report, expected in January 2017, will describe the task force history and background and will report on gaps and opportunities in the current payments landscape. The second, expected in mid-2017, will provide a discussion and assessment of the specific proposals. The second section will also identify strategic issues deemed important to the successful development of faster payments in the United States, and recommend industry actions required to advance their implementation and adoption.

For more information, contact Jeremy Mandell at jmandell@mofo.com.

PREEMPTION

One Goes One Way

Faithful readers are well aware of the conflicting decisions on the scope of FCRA preemption on state claims based on furnishing of information. A federal court in Pennsylvania dealt with this issue recently, adopting the blanket approach in finding statutory and common law claims preempted. *Prukala v. TD Bank USA*, No. 3:16-CV-0894, 2016 WL 6191912 (M.D. Pa. Oct. 24, 2016). The court recognized that the Third Circuit has not considered the issue, and district courts in the circuit have come to conflicting conclusions. The court considered earlier rulings by courts in the circuit finding statutory claims were not preempted but declined to follow them in light of more recent decisions, including decisions from the

Second and Seventh Circuits adopting the blanket approach.

For more information, contact Nancy Thomas at nthomas@mofo.com.

One Goes the Other

A federal court in Kentucky also considered the scope of FCRA preemption recently in another jurisdiction where courts have applied different approaches. *Poynter v. Ocwen Loan Servicing, LLC*, No. 3:13-cv-773-DJH-CHL, 2016 WL 5380926 (W.D. Ky. Sept. 23, 2016). The court didn't even consider the blanket approach. Instead, it considered the temporal approach, in which claims based on actions after the furnisher received notice of a dispute are preempted, but defamation, invasion of privacy, or negligence claims based on actions before the furnisher received notice are not preempted as long as the plaintiff can establish malice or willful intent to harm. The court also considered the statutory approach, in which common law claims are preempted, but statutory claims are not. The court adopted the temporal approach, finding plaintiffs' claims were preempted because they relate to the defendant's obligations after learning of the disputed information.

For more information, contact Nancy Thomas at nthomas@mofo.com.

PRIVACY

Buckle Up, New Yorkers!

On September 13, 2016, the New York State Department of Financial Services (NYDFS) proposed rules that would require financial institutions subject to NYDFS's authority to put in place cybersecurity programs that would include a number of specific controls designed to protect information systems and "nonpublic information." The proposal is quite broad and likely to create compliance challenges if adopted as proposed, given the breadth of systems and information it covers. In addition, some of the proposal's prescriptive requirements, such as encrypting all "nonpublic information" both in transit and at rest, appear to be challenging. All covered entities would also be required to report "cybersecurity events" and "material" vulnerabilities to NYDFS within 72 hours, and boards of directors would be required to provide annual certifications of compliance to NYDFS.

For more information, read our Client Alert or contact Nate Taylor at ndtaylor@mofo.com.

Big Bank Standards Considered

On October 19, 2016, the OCC, Fed, and FDIC released an Advance Notice of Proposed Rulemaking (ANPR) laying out a framework for enhanced cyber risk management standards that the agencies are considering requiring of certain "large and interconnected" financial institutions. The ANPR lays out a contemplated framework of enhanced standards, and requests comment on a series of questions that will inform a later, more specific proposal. Their initial focus is on financial institutions with total consolidated assets of $50 billion or more, including bank holding companies and banks and thrifts, though the agencies are also considering applying the enhanced standards on an enterprise-wide basis to include subsidiaries and certain nonbank entities, including certain financial market utilities and service providers.

For more information, read our Client Alert or contact Nate Taylor at ndtaylor@mofo.com.

The FTC Wants to Play Too

The FTC put up a blog post in late August about the cybersecurity framework developed by the National Institute of Standards and Technology (NIST). NIST originally developed the framework for critical infrastructure, but the FTC believes that the framework is consistent with the "process-based approach" it has taken in its data security law enforcement actions, as well as in its previous guidance to businesses, such as its Start with Security publication. The blog post indicates that the FTC believes that the five functions outlined by the framework (Identify, Detect, Protect, Respond, Recover) "signify the key elements of effective cybersecurity" and that all companies (not just critical infrastructure) can use them as a "model" for conducting risk assessments and mitigation, and then to either establish or improve their data security programs.

For more information, read our Client Alert or contact Andy Serwin at aserwin@mofo.com.

See Something, Say Something

FinCEN issued an advisory to covered financial institutions about reporting "cyber-enabled crime and cyber-events" through Suspicious Activity Reports (SARs). Specifically, a covered financial institution *must* file a SAR where it "knows, suspects, or has reason to suspect that a cyber-event was intended, in whole or in part, to conduct, facilitate, or affect a transaction or a series of transactions" because "it should be considered part of an attempt to conduct a suspicious transaction or series of transactions." The advisory provides examples of what may constitute a cyber event, such as a DDOS attack that distracts cybersecurity personnel from "immediately detecting or stopping an unauthorized $2,000 wire transfer." This

advisory comes on the heels of another advisory FinCEN issued in September "to help financial institutions guard against a growing number of e-mail fraud schemes in which criminals misappropriate funds by deceiving financial institutions and their customers into conducting wire transfers."

For more information, contact Adam Fleisher at afleisher@mofo.com.

Cyber 101

Perhaps not wanting to be left out, the Group of 7 (G-7) recently released a guidance document entitled *Fundamental Elements of Cybersecurity for the Financial Sector*. The Department of the Treasury and the Federal Reserve Board issued a press release welcoming the guidance, noting that it "provide[s] a concise set of principles on best practices in cybersecurity for public and private entities in the financial sector." The guidance, as the press release notes, focuses on eight fundamental building blocks, such as establishing a cybersecurity strategy and framework, governance, risk assessment and controls, monitoring, and incident response and recovery. It also includes information sharing and the concept of "continuous learning," which entails reviewing the cybersecurity strategy and framework regularly and as warranted.

For more information, contact Nate Taylor at ndtaylor@mofo.com.

Had a Breach? The FTC Is Here to Help

The FTC has also issued a new video and guide for businesses on "what to do when you suspect a data breach." The guide includes suggestions such as calling the local police department immediately to "[r]eport your situation and the potential risk for identity theft," and offering "at least a year of free credit monitoring or other support such as identity theft protection," and points out the importance of prompt notice to individuals. The guide also includes a number of suggestions for the notice itself, including providing information about law enforcement working on the incident and encouraging people who discover that their information has been misused to file a complaint with the FTC. Of course, any guidance from the FTC would not necessarily override obligations under state breach-notice laws with respect to the contents of any notice provided to individuals about an incident.

For more information, contact Nate Taylor at ndtaylor@mofo.com.

Don't Blame Us

As cyberattacks have become more sophisticated, and as they are more frequently perpetrated by state actors or state-sponsored actors, many in the federal government have sought to encourage collaboration in part by framing companies that get attacked as victims. For example, in September 2016, Secretary of Commerce Penny Pritzker gave a speech in which she said that while the government wants to work with private companies, "[w]e cannot blame executives for worrying that what starts today as an honest conversation about a cyberattack could end tomorrow in a 'punish the victim' regulatory enforcement action." Similarly, FBI Director James Comey recently said that the FBI does "not think of private sector partners who have been victimized by cyber intrusion any differently than [it does] a victim of a violent crime." Consumer protection regulators have not, however, been singing the same tune.

For more information, contact Andy Serwin at aserwin@mofo.com.

A New Kind of Watchdog

The California attorney general recently announced an online form intended to "help consumers report websites, mobile applications, and other online services that are in violation of" California's Online Privacy Protection Act (CalOPPA). CalOPPA generally requires that a website or mobile application that collects personal information include a privacy policy describing the categories of information collected, third-party sharing, review and access rights to personal information, and the effective date of the privacy policy. The reporting form provides checkboxes for the "nature of the alleged noncompliance." Before you turn anybody in, you should be aware that the AG thinks this tool will allow "consumers to 'crowdsource' privacy policy violations, exponentially increasing the [AG's] ability to identify and notify those in violation of CalOPPA."

For more information, contact Julie O'Neill at joneill@mofo.com.

Hostage Taking

The FTC is not only offering advice on how to deal with a breach generally, but also with how to respond to a ransomware attack. On this topic, the FTC has another blog post, which provides background on ransomware and then summarizes some suggestions from the FTC's workshop on ransomware and how to defend against it, such as training and education, good "cyber hygiene" to manage risk of exposure to malware, maintaining good backups, and having a plan to respond to an attack. For a business that is a victim, the FTC recommends that companies consider implementing their response plans, calling the FBI or other law enforcement, and containing

the attack. The blog post also notes that most panelists at the workshop, "including law enforcement, don't condone paying the ransom," though they "recognized that businesses may need to evaluate all possible options."

For more information, contact Nate Taylor at ndtaylor@mofo.com.

Dangerous Things

On a quiet Friday in mid-October, hackers successfully executed a DDOS attack that brought down large swaths of the Internet. As was widely reported, the attackers used connected devices (implicating the Internet of Things) to perpetrate the attack. How timely, then, that the National Telecommunications & Information Administration (NTIA) of the U.S. Department of Commerce announced a multi stakeholder process regarding security upgradability and patching relating to the Internet of Things. The first meeting of this process was on October 19 in Austin, Texas, to coincide with the Consumer Technology Association's Technology and Standards Forum. In announcing the process, the NTIA stated its belief that, in order for the potential of the IoT to be realized, users of IoT devices "need reasonable assurance that connected devices, embedded systems, and their applications will be secure." Recent events have likely made it easier for the NTIA to make its case about the important of Internet of Things security.

For more information, contact Nate Taylor at ndtaylor@mofo.com.

Breaches and Liability

Schnuck Markets won a significant victory in a long-running dispute with credit card issuers over its payment card breach that occurred in late 2012. *Cmty. Bank of Trenton v. Schnuck Mkts., Inc.*, No. 15-cv-01125-MJR, 2016 WL 5409014 (S.D. Ill. Sept. 28, 2016). The plaintiff financial institutions alleged 13 claims for relief, and the court dismissed all the substantive counts for failure to state a claim. The court gave particular weight to the difference between individual claimants in a data breach—who can, for example, identify tangible harms, such as fraudulent charges on their accounts—and financial institution claimants. The court found that the financial institutions' claims were "highly general" and vague, and consistently expressed skepticism that Schnucks was negligent, misrepresented its practices, or caused harm to the banks under consumer protection statutes. *Id.* at *3.

For more information, contact Nate Taylor at ndtaylor@mofo.com.

ARBITRATION

Financial Choice Act Could Impact Arbitration Rule

The proposed Financial Choice Act, H.R. 5983, seeks to significantly transform elements of the Dodd-Frank Act and the structure and powers of the CFPB. One of its provisions would thwart the CFPB's proposed arbitration rule by repealing the CFPB's authority to restrict arbitration. The Act's comprehensive summary describes the proposed arbitration rule as "misguided and burdensome." The Choice Act is sponsored by Texas Congressman Jeb Hensarling, and while the bill has not been passed, Congressman Hensarling has been quoted as noting that the recent election of Donald Trump likely increases the bill's possibility of success. We will continue to track this bill.

For more information, read our Client Alert or contact Don Lampe at dlampe@mofo.com.

Who Wears the Arbitration Hat

The Ninth Circuit dealt a blow this September to plaintiffs (Uber drivers) alleging improper use of consumer reporting information about them. *Mohamed v. Uber Techs., Inc.*, 836 F.3d 1102 (9th Cir. 2016). The Ninth Circuit overturned the district court's decision and held that an arbitrator, not the court, must decide whether all but one of the plaintiffs' claims are arbitrable. The court held the only claims for which arbitrability was *not* delegated to the arbitrator were claims under the California Private Attorney General Act, and even that carve-out was eliminated in Uber's later (and superseding) driver agreements.

For more information, contact James McGuire at jmcguire@mofo.com.

Bank Too Late to Compel Arbitration of Overdraft Cases

As part of the long saga of overdraft cases, the court held that one bank was too late to compel arbitration against absent class members after the class had been certified. *In re: Checking Account Overdraft Litigation*, No 1:09-MD-02036-JLK, 2016 U.S. Dist. LEXIS 145813 (S.D. Fla. Oct. 17, 2016). The court noted that the bank had had opportunities to compel arbitration but instead chose to litigate for years, unlike other banks that successfully moved to compel arbitration earlier. The court held that the bank's decision to file substantive motions, engage in discovery, and otherwise engage in the litigation process precluded it from now seeking to compel arbitration.

For more information, contact Natalie Fleming-Nolen at nflemingnolen@mofo.com.

TCPA

Stop It, Already

A Texas federal court held that a TCPA plaintiff had standing under *Spokeo* based on allegations that receiving multiple prerecorded messages "disrupted, inconvenienced, and agitated." *Holderread v. Ford Motor Credit Co.*, No. 4:16-CV-00222, 2016 WL 6248707, at *3 (E.D. Tex. Oct. 26, 2016). The court reasoned that "the harm caused by unwanted phone calls is closely related to an invasion of privacy, which is a widely recognized common law tort," and that "Congress identified the intangible harm of invasion of privacy as legally cognizable." *Id*.

For more information, contact David Fioccola at dfioccola@mofo.com.

Spokeo Strikes Back

A California federal court found that a consumer lacked Article III standing to assert a TCPA claim under *Spokeo* where he failed to connect his purported injury—incurring a charge for the incoming call to his cell phone—to the allegedly unlawful use of an autodialer to place the call. *Ewing v. SQM US, Inc.*, No. 3:16-CV-1609-CAB-JLB, 2016 WL 5846494, at *2 (S.D. Cal. Sept. 29, 2016). Specifically, the plaintiff "d[id] not, and [could] not, allege that the Defendants' use of an ATDS to dial his number caused him to incur a charge that he would not have incurred had Defendants manually dialed his number, which would not have violated the TCPA." *Id*. The court rejected the plaintiff's new injury allegations raised in opposition (i.e., that it had been a waste of time answering the call and depletion of his phone battery) for the same reasons.

For more information, contact Tiffany Cheung at tcheung@mofo.com.

Once Is Enough

According to a Georgia federal judge, receiving a single unwanted text message is enough to satisfy Article III's standing requirements in a TCPA action post-*Spokeo*. *Etzel v. Hooters of Am., LLC*, No. 1:15-cv-01055-LMM (N.D. Ga. Nov. 15, 2016), ECF No. 39. The court stated that "the Eleventh Circuit ha[s] held that Congress intended to create injury where the [TCPA] was violated" and "[t]his means that if the plaintiff has been personally affected by the conduct that violates the statute, standing exists." *Id*. at 6. In the context of text messages, the court found that injuries could include charges for the unwanted text, depletion of the cellphone's battery, wasted time reading and responding to the text, and an invasion of privacy.

For more information, contact David Fioccola at dfioccola@mofo.com.

This newsletter addresses recent financial services developments. Because of its generality, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.

The firm members who specialize in financial services are:

Los Angeles

Henry Fields	(213) 892-5275 hfields@mofo.com
Joseph Gabai	(213) 892-5284 jgabai@mofo.com
Robert Stern	(213) 892-5484 rstern@mofo.com
Nancy Thomas	(213) 892-5561 nthomas@mofo.com

New York

James Bergin	(212) 468-8033 jbergin@mofo.com
David Fioccola	(212) 336-4069 dfioccola@mofo.com
Mark Ladner	(212) 468-8035 mladner@mofo.com
Barbara Mendelson	(212) 468-8118 bmendelson@mofo.com
Michael Miller	(212) 468-8009 mbmiller@mofo.com
Joan Warrington	(212) 506-7307 jwarrington@mofo.com

San Francisco

Michael Agoglia	(415) 268-6057 magoglia@mofo.com
Roland Brandel	(415) 268-7093 rbrandel@mofo.com
Angela Kleine	(415) 268-6214 akleine@mofo.com
Adam Lewis	(415) 268-7232 alewis@mofo.com
Jim McCabe	(415) 268-7011 jmccabe@mofo.com
James McGuire	(415) 268-7013 jmcguire@mofo.com
William Stern	(415) 268-7637 wstern@mofo.com

Washington, D.C./Northern Virginia

Leonard Chanin	(202) 887-8790 lchanin@mofo.com
L. Richard Fischer	(202) 887-1566 lfischer@mofo.com
Oliver Ireland	(202) 778-1614 olreland@mofo.com
Don Lampe	(202) 887-1524 dlampe@mofo.com
Obrea Poindexter	(202) 887-8741 opoindexter@mofo.com

ABOUT MORRISON & FOERSTER

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on The American Lawyer's A-List for 13 straight years and the Financial Times named the firm number six on its list of the 40 most innovative firms in the United States. Chambers USA has honored the firm with the only 2014 Corporate/M&A Client Service Award, as well as naming it both the 2013 Intellectual Property and Bankruptcy Firm of the Year. Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger.

NEWSLETTER STAFF

Editor-in-Chief: Nancy Thomas

Mortgage & Fair Lending Report
Angela Kleine, Managing Editor

Beltway Report
Leonard Chanin

Bureau Report
Jessica Kaufman

Mobile & Emerging Payments Report
Obrea Poindexter and Trevor Salter

Operations Report
Jeremy Mandell

Preemption Report
Nancy Thomas

Privacy Report
Nate Taylor and Adam Fleisher

Arbitration Report
Natalie Fleming-Nolen

TCPA Report
Tiffany Cheung

Can't wait for the next issue? The Financial Services Group sends out client alerts by e-mail, reporting on developments of significance. If you would like to be added to our circulation list, contact Taylor Birnbaum at tbirnbaum@mofo.com.

If you wish to change an address, add a subscriber, or comment on this newsletter, please write to:

Taylor Birnbaum
Morrison & Forester LLP
250 West 55th St.
New York, NY 10019
tbirnbaum@mofo.com