Skadden

PRIVACY & CYBERSECURITY UPDATE

DECEMBER 2014

CONTENTS (click on the titles below to view articles)

The Critical Takeaway for Every Company From the Sony Cyber Attack 1

Sony Data Breach Class Action Complaint Provides Insight Into Cybersecurity Issues 2

Reminder: New California Data Protection Laws Went Into Effect January 1 3

New Federal Cybersecurity Laws May Create Momentum Toward More Legislation 3

NIST to Provide Guidance on Implementing its Cybersecurity Framework 6

New York Department of Financial Services Implements New Cybersecurity Examination Procedure. 7

EU's Article 29 Working Party Looks to Standardize Review of Model Contract Clauses . . . 8

Developments in the Target Lawsuits 9

Illinois Federal Court Dismisses Privacy Class Action Against P.F. Chang's for Lack of Standing 12

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on Page 13, or your regular Skadden contact.

THE CRITICAL TAKEAWAY FOR EVERY COMPANY FROM THE SONY CYBER ATTACK

This time last year, media and privacy experts were singularly focused on the cyber attack on Target and the lessons companies could learn from such a major attack. While many companies heeded these lessons, many more viewed the Target incident as inapplicable to their own businesses. In their view, since they did not have a large-scale retail presence or did not collect consumer credit card information, cyber attacks such as the one that hit Target (and many more in 2014) were problems for another industry.

Now, as 2014 draws to a close, media and privacy experts are once again singularly focused on a cyber attack, albeit one of an entirely different nature. The cyber attack on Sony is unlike any other cyber attack to date in terms of the amount of sensitive business information and communications that have been made public, the extended focus by the media, and the involvement of the White House and other government officials at the highest levels. The aftermath of the attack on Sony is, in some ways, so unique that companies are in danger of falling into the same trap as from the Target attack — namely, dismissing it as a "one-off" case with no application to their own business. Too many businesses are already rationalizing that Sony has no relevance to their own operations because they do not engage in any activity that could draw the ire of a foreign nation state with cyber attack capabilities.

The Sony cyber attack should teach companies an entirely different lesson. Target, Sony and myriad other attacks over the last two years highlight that every company is vulnerable to cyber attacks, regardless of their size, industry or the information they hold. As just one example, at Skadden, we have seen clients attacked by politically motivated hackers not because of the company's business agenda but through "ransomware" attacks, where the hackers sought money to finance their politically focused operations. Other companies have suffered the theft of valuable business information, ranging from intellectual property to confidential business plans. While each company's exposure to risk varies, no company should consider their risk exposure so low that cyber-attack preparedness is not front and center on their agenda for 2015.

In many ways, cyber-attack preparedness is a technology issue, but the companies that are best prepared for these attacks take a holistic approach, with heavy involvement from the legal department and business units. Every company's legal department should be spearheading regular privacy and cybersecurity audits in order to identify weak spots within their organization that could expose them to costly litigation or regulatory charges should an attack occur. The legal department should also coordinate the creation of a Cyberattack Response Plan (also called a Severe Incident Response Plan) that identifies (1) the roles and responsibilities of a rapid response team, (2) the response logistics and (3) key decisions to consider. Companies that develop and train staff on such plans are far better at responding quickly and effectively to cyber attacks, and in a way that minimizes their risk exposure.

SONY DATA BREACH CLASS ACTION COMPLAINT PROVIDES INSIGHT INTO CYBERSECURITY ISSUES

As has happened in nearly every cybersecurity attack, the recent attack on Sony has already generated class action litigation.[1] In this case, a lawsuit was filed on December 15, 2014, purportedly on behalf of all current and former Sony employees whose personally identifiable information (PII) was compromised in the attack. Since it is difficult to sue a company simply for being hacked, the plaintiffs, as in other cybersecurity class action lawsuits, are attempting to establish a set of steps that Sony failed to take, and that allegedly would have prevented the attack. In that respect, the complaint provides a roadmap of the types of issues plaintiffs' counsel raise when a company suffers a cyber attack.

The complaint includes four causes of action: common law negligence because Sony allegedly failed to use reasonable care to protect and secure the plaintiffs' PII, and failed to disclose the existence and extent of the data breach to the plaintiffs in a timely and accurate manner; violation of the California Confidentiality of Medical Information Act because Sony allegedly failed to secure and protect medically related PII of California class members; and violation of the California and Virginia data breach notification statutes because Sony allegedly failed to provide notice of the breach to residents of those states "without unreasonable delay."

The plaintiffs base their claims on allegations that Sony failed to meet industry standards in protecting its employees' data. The plaintiffs include excerpts from various reports and direct quotes from Sony personnel allegedly suggesting that Sony knew it was not doing enough to secure its systems. For example, the plaintiffs include a 2007 quote from Sony's executive director of information security that the company made a "valid business decision to accept the risk" of a data breach rather than improve its systems, because it felt as though the cost of notifying affected individuals of any breach was less than that of upgrading its security. Another internal Sony report, released two months before the hacking incident became public, allegedly revealed that basic security protocols were not in place at Sony, and that the security systems that were in place were unmonitored.

The plaintiffs also provide a timeline of historical data security issues experienced by Sony in an attempt to establish that Sony willfully and knowingly failed to maintain adequate data security procedures. With respect to each incident, the plaintiffs relate news reports, expert analysis or alleged Sony admissions that Sony's systems were not adequate to protect the data that was compromised.

The plaintiffs then describe areas where Sony allegedly fell short in its duty to maintain reasonable and adequate security measures, including, in the plaintiffs' view: failing to design and implement appropriate firewalls and computer systems; failing to properly and adequately encrypt data; losing control of and failing to quickly regain control over Sony's cryptographic keys; and improperly storing and retaining information on its inadequately protected network.

PRACTICE POINTS

The Sony complaint highlights that cybersecurity is not simply an IT issue. When an attack occurs, plaintiffs will look for oral and written statements by company employees — no matter how old or out of context — to try and build a case of negligence or failure to maintain reasonable and adequate security measures. A thorough cybersecurity and privacy review can help highlight these statements and introduce critical steps to take to mitigate or eliminate any risk exposure. External counsel should be considered for such reviews since they bring a wide range of "best practices" expertise.

Return to Table of Contents

[1] *Corona v. Sony Pictures Entertainment, Inc.*, 2:14-cv-09600-RGK-SH, C.D. Cal.

REMINDER: NEW CALIFORNIA DATA PROTECTION LAWS WENT INTO EFFECT JANUARY 1

On January 1, two new California laws went into effect that have ramifications for any company doing business in that state.

As we reported in our October 2014 *Privacy & Cybersecurity Update*, California law AB 1710, which went into effect January 1, seeks to improve the protection of California residents' personal information by making three changes to existing state laws concerning breach notifications and the protection of personal data:

- Broadening the obligation to implement reasonable security procedures to include not only businesses that own or license personal information, but also data brokers, third-party service providers and other businesses that "maintain" such information without owning or licensing it from others;
- Prohibiting the sale of an individual's Social Security number, except where the release of the number is ancillary to a legitimate transaction; and
- Enhancing consumer protections in the event of a data breach by requiring "the source of the breach" to "provide appropriate identity theft prevention and mitigation services, if any," at no cost to the affected person for at least one year.

As we reported in our November 2013 *Privacy & Cybersecurity Update*, starting on January 1, websites and other online or mobile services and applications that are directed at California residents under 18 years of age (minors), or are operating with actual knowledge that one or more minors are visiting or using the service, must provide minors with the ability to remove or, if the operator prefers, to request and obtain removal of, content the minor posted on the service. These registered minors must be provided with notice of this right along with clear instructions on how to remove or request removal of such content. The law also prohibits certain advertising on sites directed to minors.

Return to Table of Contents

NEW FEDERAL CYBERSECURITY LAWS MAY CREATE MOMENTUM TOWARD MORE LEGISLATION

After years of debate and discussion regarding federal information security legislation, Congress has finally taken a step in that direction with passage of the Federal Information Security Modernization Act of 2014 (FISMA),[2] the National Cybersecurity Protection Act of 2014 (NCPA)[3] and the Cybersecurity Enhancement Act of 2014 (CEA).[4] President Obama signed each bill into law on December 18, 2014. While these acts are primarily directed at the public sector and not the private sector, their enactment suggests that the logjam in enacting cybersecurity legislation may finally be breaking.

FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014

FISMA amends the Federal Information Security Management Act of 2002, and seeks to (1) provide a comprehensive framework for ensuring that information security controls over federal information are effective and (2) improve oversight of federal agency information security programs.

FISMA clarifies the roles of the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) with regard to cybersecurity. OMB is tasked with overseeing general agency implementation of information security policies and procedures, and

---

[2]Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283 (2014). The full text of the act is available at https://www.congress.gov/bill/113th-congress/senate-bill/2521/text.
[3]National Cybersecurity Protection Act of 2014 , Pub. L. No. 113-282 (2014). The full text of the act is available at https://www.congress.gov/113/bills/s2519/BILLS-113s2519enr.pdf.
[4]Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274 (2014). The full text of the act is available at https://www.congress.gov/113/bills/s1353/BILLS-113s1353enr.pdf.

ensuring that standards promulgated by the National Institute of Standards and Technology Act complement those developed for national security systems. This is consistent with OMB's general mandate of overseeing agency policy. DHS is responsible for the operational side of these issues, by administering the implementation of the various agency information security policies and practices.

Every year, the director of OMB and the secretary of DHS will submit a report to Congress detailing the effectiveness of such policies and procedures. The report, compiled from information submitted by the agencies, will include a summary of the incidents during the previous year, a description of the threshold for reporting major incidents, and an assessment of agency compliance with the standards and data breach notification policies issued by the OMB director.

FISMA outlines the responsibility of each federal agency on cybersecurity. Agency heads will be responsible for ensuring that the information security protections for their agency reflect the risk and magnitude of the harm that may come from unauthorized access of information in their systems. They are also tasked with ensuring that information security management is within the agency's budget, gathering information needed to assess the risk level of the information the agency gathers, testing the information security system, and ensuring the agency has trained personnel who are able to ensure compliance with FISMA.

Agencies must develop an agencywide information security program that allows for periodic risk assessment and contains cost-effective policies that will reduce the risk to information security to an acceptable level. If an agency's information security policies and procedures will affect communication with the public, the agency is required to notify the public and provide an opportunity to comment upon the proposed procedures. Agencies must provide security awareness training to their personnel and contractors and test the effectiveness of their policies on at least an annual basis. An independent external auditor will conduct an independent evaluation of each agency's information security program on a yearly basis. Finally, in the event of a major incident, agencies must notify various committees of Congress.

FISMA requires the continuing operation of a federal information security incident center established under the 2002 act to provide agencies with technical assistance regarding security incidents and data compilation and analysis. The information center will also inform agencies of current threats and vulnerabilities and consult with the National Institute of Standards and Technology regarding information security incidents.

FISMA requires the director of OMB to ensure that data breach notification policies are periodically updated. In addition, various committees of Congress must be provided with notification of a data breach within 30 days after an agency discovers the unauthorized access or breach. Within one year, OMB must revise the OMB Budget Circular A-130 (Management of Federal Information Resources) to eliminate wasteful reporting about cybersecurity matters. For a number of years, Circular A-130 has been viewed as an inefficient and cumbersome mechanism for reporting on such matters.

NATIONAL CYBERSECURITY PROTECTION ACT

The NCPA is designed to increase information sharing between government entities and the private sector. The bill (1) codifies the Department of Homeland Security's existing National Cybersecurity and Communications Integration Center, (2) creates a federal data breach notification law when a federal agency is breached and (3) directs the undersecretary of the DHS to establish cyber incident response plans.

Though focused on cross-sector information sharing, the NCPA does not grant authority to promulgate rules or to set standards applicable to private entities relating to cybersecurity. Instead, the emphasis is on coordinating efforts to combat cyber attacks and related risks;

indeed, Congressional members lauded the bipartisan bill as the most important cyber bill to pass Congress in the last decade. According to Senate Committee on Homeland Security and Governmental Affairs Chairman Tom Carper (D-Del.), "by codifying the Department of Homeland Security's existing cybersecurity operations center, the National Cybersecurity Protection Act of 2014 bolsters our nation's cybersecurity while providing the department with clear authority to more effectively carry out its mission and partner with private and public entities."[5]

THE NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

The NCPA codifies the existing National Cybersecurity and Communications Integration Center (the Center) within DHS. The Center is a cyber and communications infrastructure that aims to reduce and manage cybersecurity breaches that threaten the country through information sharing, cyber situational awareness and incident response.[6] Under the NCPA, the Center will be a federal-civilian interface for cross-sector information sharing, composed of appropriate federal and non-federal entities. Its representatives will include elements of the federal intelligence community, federal agency members and certain nonfederal entities such as owners and operators of critical information systems. Within 180 days of the bill's enactment, the secretary of the DHS must submit recommendations to various congressional committees addressing how to expedite information-sharing agreements for cybersecurity purposes between the Center and nonfederal entities. The NCPA directs the Center to perform various services in addition to coordinating information exchange, including providing technical assistance, risk management guidance and incident response support to federal and nonfederal entities. Additionally, the NCPA imposes obligations on the DHS secretary to submit to certain congressional committees assessments of the Center's capability, its personnel composition, its privacy policies and the extent of its information sharing with each critical infrastructure sector.

FEDERAL AGENCY DATA BREACH NOTIFICATION LAW

The NCPA imposes two new notification requirements on federal agencies. First, federal agencies must notify affected individuals of a data breach involving a federal agency. The NCPA requires the notification be performed promptly after the agency discovers the unauthorized acquisition or access, though it allows for the U.S. attorney general, the head of an element of the intelligence community or the secretary of the DHS to delay notification to avoid obstructing an investigation or endangering national security or security remediation efforts. Second, the NCPA requires federal agencies affected by a data breach to notify certain congressional committees "expeditiously and not later than 30 days" following the discovery of a breach.[7]

DEVELOPMENT OF CYBER INCIDENT RESPONSE PLANS

The NCPA directs the undersecretary of the DHS, in coordination with appropriate federal departments and agencies, state and local governments, critical infrastructure sector coordinating councils, information-sharing and analysis organizations, and owners and operators of critical infrastructure, to develop and regularly update, maintain and test cyber incident response plans to address cybersecurity risks to critical infrastructure.

CYBERSECURITY ENHANCEMENT ACT OF 2014

The Cybersecurity Enhancement Act of 2014 looks to further the voluntary partnership between the public and private sectors to strengthen cybersecurity research, development, education, public awareness and preparedness. Enacted as five separate titles, the goal of the CEA is to increase collaboration, research and development, education and awareness regarding cybersecurity, and to improve technical standards.

---

[5] See http://www.hstoday.us/briefings/daily-news-analysis/single-article/congress-approves-cybersecurity-legislation/dcca3f20b55482c5fc6e2fcc4535e914.html.
[6] More information about the Center may be found at http://www.dhs.gov/about-national-cybersecurity-communications-integration-center.
[7] See *id.*

CEA encourages public and private collaboration by giving the National Institute of Standards and Technology (NIST) the task of coordinating with industry leaders and agency heads to develop cost-effective technical standards designed to guide individuals who own or oversee critical infrastructure in managing their cybersecurity risks. While these measures are voluntary, CEA calls for them to align with international standards to the fullest extent, avoid duplicating regulatory processes already in place, incorporate industry best practices, and mitigate the impact on business confidentiality, individual privacy and civil liberties.

CEA bolsters cybersecurity by calling upon the National Science and Technology Council and the Networking and Information Technology Research and Development Program to develop a strategic plan that will build upon existing cybersecurity research and development programs. The objectives of the plan include (1) designing software-intensive programs that are secure and reliable when first deployed, (2) testing of internally developed and third-party software to ensure it is free of security flaws and is properly functional, and (3) guaranteeing the privacy of individuals. The strategic plan will include near-term, mid-term and long-term goals and focus on how to translate the research into applicable new cybersecurity technology. Agencies are required to collaborate with existing industry, academia and other interested stakeholders to ensure that the efforts are not duplicative of private sector efforts.

The director of the National Science Foundation (NSF) and the director of the Office of Science and Technology Policy will review the existing cybersecurity test beds and determine whether there are enough to meet the current federal need. If more test beds are needed, they will be established at qualified institutions of higher education and nonprofits. The research under CEA will be coordinated with ongoing research being conducted by other governmental agencies. The NIST director also must develop security automation standards to minimize security risks.

CEA also looks to improve the development of future cybersecurity and technology professionals. The law contains an initiative to integrate cybersecurity practices into the core curriculum of computer science programs and requires several agencies to support competitions geared toward recruiting talented individuals. The NSF director will establish a scholarship program to develop information technology professionals and security managers, and the winners will commit to work on cybersecurity issues for the government for a set period of time.

The NIST director also will work in conjunction with various other federal agencies to continue the ongoing National cybersecurity awareness and education program to promote the widespread dissemination of technical standards, to make best practices usable by smaller entities, to support formal education programs and to increase public awareness of cybersecurity and safety issues. In addition, the NIST director will be tasked with developing international technical standards related to information system security, implementing a cloud computing strategy for the federal government and increasing interoperability among identity management technologies to improve privacy protection and usability.

Return to Table of Contents

NIST TO PROVIDE GUIDANCE ON IMPLEMENTING ITS CYBERSECURITY FRAMEWORK

In February 2014, the National Institute of Standards and Technology (NIST) released its "Framework for Improving Critical Infrastructure Cybersecurity." Click here for our description of the Framework. The Framework was developed in response to President Barack Obama's Executive Order 13636 directing NIST to work with industry stakeholders to develop standards for defending against cyber attacks. Although the standards are voluntary, given the dearth of any other "official" pronouncement on cybersecurity preparedness, they have become the de facto standard for many companies, including those outside of the critical infrastructure space. Companies have reported to us that regulators are also increasingly relying on the Framework as a guideline to assess a company's cybersecurity preparedness.

Given this increasing focus, and consistent with its commitment that the Framework would be a "living" document, NIST released a Request for Information (RFI) on August 26 and held a Framework Workshop in October 2014. Based on the feedback it received, in early December, NIST released an update that set forth the future path for the Framework. The general consensus that emerged from this process was that more should be done to promote awareness and adoption of the Framework through government- and industry-led efforts. The NIST December statement included the following key points and observations:

- The Framework includes three components: the Core, the Profile and the Implementation Tiers. Of these components, the Implementation Tiers appear to be the least used because companies need additional guidance on how to apply them. NIST acknowledged the need for further clarification in this area, including by providing case studies and real world examples. NIST therefore announced that a priority will be to develop information and training materials that promote use of the Framework, including "actual or exemplary illustrations" of how organizations practically implement the Framework.
- NIST will not be updating the Framework within the next year to give companies time to understand and implement the current version. NIST will, however, be issuing guidance in areas such as how to productively use Framework tiers, how the Framework can be a cost-effective tool in addressing cybersecurity risks, and how the Framework's approach to cybersecurity risk management can be integrated with an organization's broader risk management processes, assessments and decision making.
- A common theme at the NIST meetings (and as noted above, an issue we at Skadden have heard from our own clients) is that "regulating agencies or Congress will make the Framework mandatory and turn it into a compliance mechanism." As a result, NIST received many requests to explain to regulators that the Framework is not designed to create additional regulations, and that regulators should make clear statements about the voluntary nature of the Framework.

Return to Table of Contents

NEW YORK DEPARTMENT OF FINANCIAL SERVICES IMPLEMENTS NEW CYBERSECURITY EXAMINATION PROCEDURE

On December 10, 2014, the New York Department of Financial Services (DFS) released a letter announcing that it is updating its information technology examination procedures to include a more robust examination of financial services institutions' approach to cybersecurity. The letter, directed to New York charter or licensed banks that come under DFS' jurisdiction, is consistent with DFS' core mission of ensuring that financial regulations keep pace with the rapidly evolving financial services industry. Benjamin M. Lawsky, superintendent of DFS, stated that hacking is a threat to the financial lives of individual consumers and to the financial market as a whole. In the guidance letter sent to DFS-regulated banks, DFS called upon financial institutions to begin thinking of cybersecurity as "an integral aspect of their overall risk management strategy" rather than just an IT function.

DFS will be adding new categories and questions to its pre-examination "First-Day Letters" that focus on IT and cybersecurity. During examinations, DFS will focus on corporate governance and reporting structures, detection and response procedures to cybersecurity threats, personnel training, information security testing, management of third-party vendors, cyber insurance and other topics. Many topics covered by DFS track the cybersecurity questionnaire that the Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) issued earlier this year. (See our April 2014 *Privacy & Cybersecurity Update*.)

DFS also is updating its examination process, including the procedure for assessing and scheduling IT/cybersecurity examinations. As part of its assessment, DFS provided a list of a dozen questions it will be asking, including requests for:

- The CV and job description of the current chief information security officer (or other individual responsible for information security), as well as a description of that individual's information security training and experience.
- Identification of all reporting lines for that individual, including all committees and managers.
- An organization chart for the institution's IT and information security functions.
- A description of how data classification is integrated into information risk management policies and procedures.
- A description of how information security is incorporated into Business Continuity Planning.
- A description of any significant changes to the institution's IT portfolio over the last 24 months from mergers, acquisitions, or the addition of new business lines.

The DFS letter is yet another example of how regulators are making cybersecurity a focal point of their examination and assessment processes.

Return to Table of Contents

EU'S ARTICLE 29 WORKING PARTY LOOKS TO STANDARDIZE REVIEW OF MODEL CONTRACT CLAUSES

On November 26, 2014, the Article 29 Working Party (the Working Party), which is primarily comprised of representatives of the data protection authority (DPA) of each EU member state, outlined a new cooperation procedure intended to standardize how the adequacy of data protection clauses are assessed.[8]

Today, most companies that transfer personal data out of the EU satisfy the "adequacy" requirement of the EU Data Directive by relying on "Model Clauses" — form agreements provided by the EU. By using these agreements, companies can transfer data to an entity located outside of the EU, even if that entity is in a country whose data protection laws are not deemed "adequate" by the EU. Most countries of the world, including the U.S., do not meet the adequacy requirement. The EU has provided model contracts for transfers between data controllers and data processors, between data controllers, and from a data processor to a sub-processor.

When companies use their own agreements to accomplish this goal or make modifications to the Model Clauses, they historically had to obtain approval from the DPA of each country whose citizens' data was processed. This meant that a company could face the bureaucratic nightmare of having the same contractual language approved by certain countries and rejected by others. This defeated the unifying purpose of having Model Clauses.

In order to address this issues, the Working Party has created a more streamlined process. Under the new cooperation procedure, a company seeking to have its clauses approved undertakes the following steps:

- Identifies a particular state's DPA to be the lead regulator;
- Asks the lead DPA to launch an EU cooperation procedure to obtain a "common point of view" on the contract; and

[8]The working document outlining the cooperation procedure can be found at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp226_en.pdf.

- Sends a copy of the contract (also in an electronic version enabling copy/paste) indicating the reference number of the utilized Model Clauses and highlighting any divergences and additional clauses. The company also must indicate the list of European Economic Area (EEA) countries from which it will be carrying out the transfers

The Working Party also provides guidance on selecting a lead DPA. Such DPA must be from a country from which the data transfer is taking place, and its selection should take into account: the location from which the contractual clauses "are decided and elaborated"; the location where processing decisions are made; the most convenient location for the processing of the request in terms of administrative burden; the EU member states from which the most data transfer will occur; and, the location of a company's European headquarters. The requested regulator is free to decline, in which case the request will be transferred to, and handled by, a different state's regulator.

After a DPA accepts or is assigned the position of lead regulator, that DPA will launch an EU cooperation procedure. The procedure involves three phases:

- *Review Process*. The lead regulator will review the contract and draft an opinion letter on whether the contract conforms to the model clauses. Depending on the number of states from which transfers will take place, one or two other DPAs will review and comment on the draft opinion.
- *Cooperation With Other DPAs*. Following the review, the proposed contract, the draft letter and any comments will be forwarded to other DPAs in the relevant member states. The Working Party's proposal includes a "Mutual Recognition" system in which participating DPAs acknowledge and agree with a lead DPA's opinion. Non-participating DPAs may similarly agree without comment or can provide comments to the draft opinion within a month's time of receiving it.
- *Finalize and Sign the Draft Letter*. If all relevant DPAs agree with the draft opinion, the lead DPA will sign the opinion on behalf of the DPAs and send the letter to the company.

While there is still a fair amount of bureaucracy in the new process, companies that have tried to align the varied opinions they have received from DPAs will welcome this change. Whether the advisory cooperation procedure will be effective in promoting a "common view" of a contract across EU member states remains to be seen. If the DPA's opinion letter indicates a company's contract is in conformity with the model clauses, the company must then contact the relevant DPAs to request official authorization. DPAs will weigh the cooperation procedure's recommendation in making their decisions but are under no obligation to rule in line with the lead DPA's decision. Nevertheless, the cooperation procedure underlines the EU's emphasis on the importance of data protection and the desire to standardize its enforcement across its member states.

Return to Table of Contents

DEVELOPMENTS IN THE TARGET LAWSUITS

In a pair of rulings on December 2 and 18, 2014, in *In re: Target Corporation Customer Data Security Breach Litigation,*[9] Judge Paul Magnuson granted in part and denied in part Target's motions to dismiss claims brought by financial institutions and a putative class of consumers against Target based on the 2013 data breach involving the theft of millions of consumers' credit card information. In allowing the financial institutions' claims to proceed, the U.S. District Court for the District of Minnesota focused on actions by Target that allegedly reduced its data security, and on Target's alleged failure to respond swiftly to alleged warning signs of an impending cyber attack. In its separate ruling in the consumer class action, the court took a very liberal approach to Article III standing and pleading standards under Rule 8(a) and 9(b) of the Federal Rules of Civil Procedure.

[9]MDL No. 14-2522 (PAM/JJK).

The *Target* opinion regarding claims brought by financial institutions underscores the need for companies to have rapid response plans and teams in place to quickly respond to the first signs of a data breach. In addition, the court's ruling regarding the consumer class action claims is likely to embolden the plaintiffs' bar in bringing class claims against defendants struck with data breaches in 2015. If other federal courts adopt a similar approach at the pleading stage, the ruling could place increased importance on the development of defenses to class certification.

BACKGROUND

In December 2013, Target announced that over a period of more than three weeks during the holiday shopping season, computer hackers stole credit and debit card information for approximately 110 million Target customers by installing malware on Target's computer servers. Lawsuits were filed on the heels of the announcement and consolidated into a multidistrict litigation. The multidistrict litigation consists of two types of claims: those brought by consumers, and those brought by financial institutions who provided credit to consumers and issued their payment cards. In separate motions, Target moved to dismiss both sets of claims.

THE FINANCIAL INSTITUTIONS RULING

In a December 2, 2014, ruling applicable to the claims by financial institutions, the court granted in part and denied in part Target's motion to dismiss claims of negligence, violation of Minnesota's Plastic Card Security Act, negligence per se, and negligent misrepresentation brought by financial institutions against Target.

Negligence Under Minnesota Law

In holding that the financial institutions had adequately pled a claim for negligence, the court focused on the issue of duty. Minnesota law generally recognizes two types of duty: (1) "general" negligence, which imposes a general duty of reasonable care under certain circumstances when the defendant's conduct creates a foreseeable risk of injury to a foreseeable plaintiff; and (2) liability for the conduct of a third party where the plaintiff and the defendant stand in a "special relationship." Target argued that a "special relationship" between it and the financial institutions was required because the harm was caused by criminal hackers. Plaintiffs argued that principles of general negligence applied because Target turned off certain features of its security measures that created a foreseeable risk of the breach of security that occurred, and plaintiffs were the foreseeable victims of that harm.

The court agreed with the plaintiffs, emphasizing Target's conduct in allowing the harm to occur, *i.e.*, disabling one of the security features that allegedly would have prevented the harm. The court also pointed to Target's alleged failure to heed warning signs as the attack began. The court further noted that imposing a duty on Target would support Minnesota's policy, expressed in Minnesota legislation, of punishing companies that failed to secure consumers' credit and debit card information.

Plaintiffs' Negligent Omission Claim

The plaintiffs also claimed that Target had a duty to disclose material weaknesses in its data security systems and procedures and failed to do so. Target attacked the claim by asserting, in part, that it had no duty to disclose to the plaintiffs, and that the plaintiffs failed to plead reliance.

The court held that the plaintiffs plausibly stated a duty to disclose since they alleged that (1) Target knew facts about its ability to repel hackers that the plaintiffs could not have known, and (2) Target's public representations about its data security practices were misleading.

The plaintiffs also asserted that actual reliance need not be pled where the allegation is fraud by omission. The court disagreed but granted the plaintiffs leave to amend to add a reliance claim.

Minnesota Plastic Card Security Act and Negligence Per Se Claims

The plaintiffs alleged that Target violated Minnesota's Plastic Card Security Act (PCSA), which forbids an entity that accepts a credit or debit card from retaining card data for more than 48 hours after authorizing the transaction. Target argued that (1) the PCSA only applied to transactions that occur in Minnesota and therefore did not apply to the majority of the transactions of which plaintiffs complained; and (2) because plaintiffs' data was stolen at the time the credit cards were swiped, and not from any database maintained by Target, whether or not Target held the data for more than 48 hours was irrelevant.

The court rejected both of Target's arguments. First, the court held that the PCSA applies to any entity conducting business in Minnesota, even if the actual transactions did not take place there. Second, the court held that the plaintiffs adequately stated a PCSA violation by claiming that the hackers had actually retrieved card security codes from Target's servers, not at the point of purchase.

THE CONSUMER CLASS ACTION RULING

In a separate December 18, 2014, ruling in the consumer class action, the court granted in part and denied in part Target's motion to dismiss claims for violations of the consumer protection laws of 49 states and the District of Columbia, violation of the data breach statutes of 38 states, negligence, breach of implied contract, breach of contract, bailment and unjust enrichment brought by 114 named plaintiffs on behalf of a putative class of Target consumers.

Plaintiffs Adequately Alleged Standing

The court rejected Target's argument that the consumer plaintiffs failed to plead actual or imminent injuries, holding that the plaintiffs' allegations of unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees constituted injury in fact sufficient to confer standing under Article III of the U.S. Constitution.

The court also denied Target's argument that state law claims from five states should be dismissed because none of the 114 named plaintiffs come from those jurisdictions. Recognizing a split of authority, the court held that the standing of named plaintiffs need not be addressed at the motion-to-dismiss stage (as opposed to the class certification stage). The court also was swayed by the fact that consumers in those states were affected by the breach even if they were not represented by the 114 named plaintiffs.

Finally, Target argued that the consumer plaintiffs lacked standing to seek injunctive relief because they did not allege ongoing or impending future harm. The plaintiffs sought injunctive relief, including an order requiring Target to (1) encrypt customers' data at its point of sale, (2) comply with federal and Minnesota law regarding data security and retention of data, (3) adopt EMV chip technology for Target-issued credit and debit cards, and (4) provide extended credit-monitoring services to plaintiffs and class members. The court held that the plaintiffs plausibly pled that their injuries would be redressed by the injunctive relief sought.

State Consumer Protection Claims

The consumer plaintiffs claimed that Target violated consumer protection statutes by (1) failing to maintain adequate data security practices, (2) failing to disclose that it lacked adequate safeguards to protect customers' financial information, (3) failing to timely disclose the data breach, and (4) continuing to accept plaintiffs' credit and debit card payments after it knew or should have known of the data breach and before it purged the malware.

The court rejected Target's argument that claims under 18 of the state statutes should be dismissed for failure to plead a duty to disclose, holding that the allegation that Target continued to accept cards after knowing of the breach was sufficient. The court did dismiss various other state claims either because they did not provide a private cause of action or because they prohibited class actions.

Data Breach Notice Claims

The plaintiffs alleges that Target violated the data breach notice statutes of 38 states by failing to provide timely and accurate notice of the breach. The plaintiffs claimed that if they had known about the breach, they would not have shopped at Target. Target argued that the plaintiffs had not established that they shopped at Target after the breach took place. The court dismissed Target's argument as premature on a motion to dismiss, holding that discovery would flesh out whether plaintiffs could sustain a "would not have shopped" claim. The court did, however, dismiss data breach notification claims in states that provided no private right of action.

State Law Negligence Claims

Plaintiffs argued that Target had a duty to (1) exercise reasonable care in securing plaintiffs' personal and financial information from being compromised and misused, and (2) timely notify the plaintiffs that their data had been or was reasonably believed to have been compromised. Target did not contest that it owed these duties, but argued that plaintiffs failed to allege any damages caused by breaches of the alleged duties. Alternatively, Target claimed that the economic loss rule barred negligence actions in several states.

Referring to its analysis of Article III standing and plaintiffs' claims under consumer protection statutes, the court held that plaintiffs adequately pled injury. The court also found that plaintiffs' allegation that, if they had known of the breach, they could have taken appropriate measures to avoid unauthorized charges, such as by changing passwords or obtaining credit monitoring services, sufficiently stated damages flowing from the alleged delay. The court did, however, dismiss the state claims in those states that rely on the economic loss rule.

PRACTICE POINTS

The court's ruling that the consumer plaintiffs adequately alleged Article III standing because they incurred unauthorized charges and other out-of-pocket expenses is consistent with the trend in the courts to find standing where some economic loss is alleged. Nevertheless, the court's ruling is likely to embolden the plaintiffs' bar, given the court's lax standards approach at the pleading stage. In addition, the court's willingness to allow questionable state law claims to proceed to discovery absent dispositive authority precluding the claim is likely to place added pressure on the class certification stage.

Return to Table of Contents

ILLINOIS FEDERAL COURT DISMISSES PRIVACY CLASS ACTION AGAINST P.F. CHANG'S FOR LACK OF STANDING

In *Lewert v. P.F. Chang's China Bistro, Inc.*,[10] Judge John Darrah granted defendant P.F. Chang's motion to dismiss claims of implied breach of contract and violation of Illinois Consumer Fraud and Deceptive Business Practices Act[11] brought by two consumers arising from a data breach that P.F. Chang's suffered that led to the disclosure of consumer credit and debit card information. The U.S. District Court for the Northern District of Illinois agreed with P.F. Chang's that plaintiffs failed to allege standing.

The plaintiffs claim they suffered four types of harms caused by the data breach: (1) overpayment for products and services purchased from P.F. Chang's, (2) monetary losses arising from unauthorized bank account withdrawals and/or related bank fees, (3) opportunity cost and value of time spent monitoring financial and bank accounts, including the cost of obtaining replacement cards, and (4) costs associated with identity theft and increased risk of identity theft.

[10]Case No. 14-cv-4787, consolidated with *Kosner v. P.F. Chang's China Bistro, Inc. No. 14-cv-4923 (JWD) (E.D. Ill. Dec. 10, 2014).*
[11]Plaintiffs also included substantially similar consumer fraud laws in other states on behalf of the corresponding classes.

The plaintiffs argued that they overpaid for food since the cost of the food implicitly included the cost of data protection — a function P.F. Chang's failed to provide. The court rejected this argument because the plaintiffs failed to plead that P.F. Chang's charged a higher price for meals paid with credit or debit cards. Similarly, the court held that the plaintiffs failed to allege that they suffered any unreimbursed charges to their credit or debit cards.

One plaintiff claimed that he suffered damages because he was unable to accrue reward points on the affected debit card for two to three days after he canceled the card with the potentially stolen information. The court noted that he did not allege that he would have actually used the debit card during this brief period, and that "simply being without a debit card" is not a cognizable injury.

Finally, relying on *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013), the Court held that speculation of future harm does not constitute actual injury. Here, speculation of possible future identity theft was insufficient to establish any injury in fact, and did not qualify as actual damages under *Clapper*.

The plaintiffs have appealed the district court's ruling to the Seventh Circuit. We note that the district court's reading of *Clapper* appears to diverge from that of other courts. For example, in the Adobe Systems Privacy Litigation case, the court concluded that plaintiffs sufficiently alleged a "certainly impending" threat of future harm by pleading that hackers targeted a company's network to steal personal information, successfully stole the information, and disseminated some of that information on the Internet. We will continue to monitor the case and its impact on future data breach litigation.

Return to Table of Contents

SKADDEN CONTACTS

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Timothy A. Miller
Partner / Palo Alto
650.470.4620
timothy.miller@skadden.com

Timothy G. Reynolds
Partner / New York
212.735.2316
timothy.reynolds@skadden.com

Michael Y. Scudder
Partner / Chicago
312.407.0877
michael.scudder@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Joshua F. Gruenspecht
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000