Locke Lord LLP

PRIVACY & CYBERSECURITY NEWSLETTER

MAY 2017

Important Initiatives at Locke Lord – NYDFS & GDPR

There have been a number of significant developments in privacy and information security law in recent months. The Privacy & Cybersecurity Group of Locke Lord LLP invests significant time to stay on top of these developments and position ourselves to efficiently help clients adapt to changing requirements. We would like to call your attention to two initiatives in particular:

- **New York Department of Financial Services Cybersecurity Regulation Initiative** - A team of our attorneys, headed by Ted Augustinos and Pat Hatfield, have closely followed developments and issues relating to the cybersecurity regulation recently promulgated by the New York Department of Financial Regulation. As you may know, this new regulation imposes highly particularized requirements, and will necessitate significant actions by many covered entities. Our team is working to develop guidance, language, and strategies to help entities come into compliance in ways that will be practical and provide appropriate security.
- **EU General Data Protection Regulation Initiative** - Our GDPR initiative is headed by Tom Smedinghoff, and is spearheading the Privacy & Cybersecurity Group's efforts to prepare clients for the significant legal changes approaching with respect to EU personal data. These efforts include careful study of GDPR issues, and development of practical guidance for entities dealing in or with European personal data.

Please contact the leaders of these initiatives, or anyone on our team, if you would like to discuss how we can help your organization with these changing laws.

IN THIS ISSUE

Locke Lord LLP

Locke Lord's Privacy & Cybersecurity Newsletter provides topical snapshots of recent developments in the fast-changing world of privacy, data protection and cyber risk management. For further information on any of the subjects covered in the newsletter, please contact one of the members of our privacy and cybersecurity team.

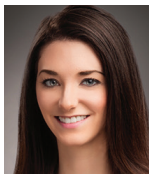
OUR AUTHORS:

Sean Kilian
Associate
Dallas
214-740-8560
skilian@lockelord.com

Glenn G. Pudelka
Counsel
Boston
617-239-0371
glenn.pudelka@lockelord.com

Charles M. Salmon
Senior Counsel
Austin
512-305-4722
csalmon@lockelord.com

Molly McGinnis Stine
Partner
Chicago
312-443-0327
mmstine@lockelord.com



Ashley Wheelock
Associate
Austin
512-305-4860
ashley.wheelock@lockelord.com

Tammy Ward Woffenden
Partner
Austin
512-305-4776
twoffenden@lockelord.com

Bilal Zaheer
Partner
Chicago
312-201-2875
bilal.zaheer@lockelord.com

"If At First You Don't Succeed…" - Shareholders Keep Trying to Sue Ds&Os for Data Security Breaches

Several high-profile lawsuits have been filed in recent years by shareholders seeking to hold corporate officers and directors liable for damage resulting from data security breaches. For example, directors and officers at Target (2014), Wyndham Hotels (2014), and Home Depot (2015) faced such shareholder derivative actions in connection with data breaches experienced by those companies.

So far, these cases have all ended the same way: the trial court dismissed the shareholders' complaint for failure to allege facts sufficient to overcome initial pleading hurdles, such as demand futility and the business judgment rule.

In light of this string of dismissals, one might be tempted to conclude that shareholders would give up on pursuing directors and officers in the wake of a data breach.

But two recently-filed shareholder suits, against Wendy's and Yahoo!, show that, despite mounting unfavorable court rulings, the plaintiffs' bar persists in searching for ways to crack the judicial code and plead viable D&O claims stemming from data security breaches. Thus, the potential for D&O liability resulting from data breaches and the defense costs associated with the cases should remain a concern for insurers and corporations alike.

On December 16, 2016, a Wendy's shareholder initiated a derivative lawsuit in the federal district court for the Southern District of Ohio against the company and nineteen of its directors and officers for liability from a data security breach. Wendy's began investigating a potential data breach in early 2016, after learning of unusual activity at one of its restaurants. In a series of public disclosures stretching from February to July 2016, the company stated that it had discovered certain malware had been installed in point of sale systems used at over 1,000 Wendy's restaurant locations, and as a result, the personal and financial information of Wendy's customers had been compromised between October 2015 and June 2016. Similar to the complaints filed against Target, Wyndham and Home Depot, the complaint against Wendy's asserts claims for breach of fiduciary duty, corporate waste, unjust enrichment and "gross mismanagement" in connection with the data breach.

No doubt to avoid a fate similar to that of the shareholder suits against Target, Wyndham, and Home Depot, the plaintiff in the Wendy's case has made a concerted effort to plead allegations sufficient to demonstrate demand futility. For example, the complaint alleges that a group of the defendants owns enough stock to command a controlling interest in the company and that a number of defendants have familial ties or other connections to the controlling defendants such that they are "beholden to the controlling shareholder defendants" and ostensibly incapable of impartially considering a demand to sue. The defendants have moved to dismiss on several grounds, including failure to adequately plead demand futility. Wendy's, like Wyndham and Home Depot, is a Delaware corporation, and thus, the written opinions in those two cases (both of which were cited in the defendants' motion to dismiss) are likely to be particularly instructive to the Ohio district court. It remains to be seen whether the facts of this case are sufficiently distinguishable for the plaintiff to avoid dismissal.

On February 21, 2017, shareholders of Yahoo! filed a derivative lawsuit in Delaware chancery court against the company's CEO, one of its co-founders, and the chairman of its board, among others. The shareholder suit is the latest in a series of lawsuits filed against Yahoo! stemming from the company's late 2016 disclosures that it was hacked on two separate occasions in 2013 and 2014, resulting in the theft of personal information belonging to over 1.5 billion Yahoo! users. In its 2016 Annual Report, Yahoo! reported that "43 putative consumer class action lawsuits have been filed against the Company in U.S. federal and state courts" relating to the data breaches. Though the Delaware shareholder complaint is sealed, related court filings indicate that the lawsuit alleges breach of fiduciary duty claims against the defendants relating to the non-disclosure of the data security breaches, making it similar to the lawsuits filed against Target, Home Depot, Wyndham and Wendy's.

Though the case was only recently filed and the complaint has not yet been tested by a motion to dismiss, the Yahoo! case may stand the best chance yet of surviving the pleading stage. To begin with, the sheer size of the breach (over 1.5 billion compromised accounts), the time between the breach and public disclosure (between two and three years) and the fact that Yahoo! is a technology company whose core business is providing email accounts secured by passwords may be enough to support a claim that the defendants breached their fiduciary duties in preventing, detecting and remedying the data breach. Furthermore, as disclosed in the company's annual report, an independent committee formed by the Yahoo! board, and assisted by independent counsel as well as a forensic expert, conducted an investigation and issued a report concluding, among other things, that "certain senior executives did not properly comprehend or investigate, and therefore failed to act sufficiently upon, the full extent of knowledge known internally" relating to the data breaches. This is in contrast to the Target case, where a Special Litigation Committee issued a ninety-one page report recommending that the company not pursue D&O litigation, which report included detailed findings on the steps the company took to implement security measures pre-breach and to remedy the breach once it was discovered.

The Wendy's and Yahoo! suits serve as a reminder that, even though courts have thus far dismissed D&O suits stemming from data breaches, plaintiffs continue to file these suits. And the specter of D&O defense costs and liability remains.

Testing the Limits II – Cyber Coverage Litigation Keeps on Rolling

As cyber risks continue to evolve, resulting insurance claims continue to implicate a variety of types of policies. Although many claims are addressed without lawsuits being filed, some are not. And while not all coverage actions result in a substantive litigation decision, some do. As those decisions accumulate, they are worth examining as this very active area of risk management grows.

One of the most talked-about types of cybercrime remains "business email compromises." These measures are designed to hoodwink people into sending or releasing funds to someone other than the intended recipient. Cases continue to be litigated over whether policies with computer fraud, funds transfer fraud, crime or other coverages respond to such losses of funds. Recent

decisions show the importance of specific policy language and the particular facts of the schemes or scams.

In Taylor and Lieberman v. Federal Ins. Co., the federal 9th Circuit Court of Appeals affirmed summary judgment in favor of the insurer on March 9, 2017. The policyholder, an accounting firm, was hit by a fraudster who took control of the email account of one of the firm's clients. The perpetrator used the client's account to send seemingly legitimate wire payment instructions and backup documentation to the policyholder. After twice arranging for wire transfers in response to such communications, an employee of the policyholder contacted the client for confirmation before accommodating a third request. The plan was exposed, additional funds were not sent to the false account, and some of the earlier-sent money was recovered. The accounting firm sought coverage for the balance under a portfolio policy with forgery, computer fraud, and funds transfer fraud coverage sections.

In granting summary judgment for the insurer, the *Taylor and Lieberman* trial court noted that a "direct loss" is required for coverage but was absent in this case. The court remarked that a "direct loss" might have been something like the draining of funds from an escrow account maintained by the policyholder and hacked into by the perpetrator. Instead, said the court, this loss resulted from "a series of far more remote circumstances…."

The appellate court affirmed on other grounds. It held that the forgery section did not apply because no financial instruments were involved. The computer fraud section was not triggered because just sending an email is not a sufficient use of a computer and there was no effort to infiltrate or affect the policyholder's system. Finally, no coverage was provided by the funds transfer fraud section because the wire transfer requests were known to and in fact arranged by policyholder and since the fraudulent instructions came to the policyholder and not a financial institution, as required by the policy.

See also InComm Holdings, Inc. v. Great Am. Ins. Co., No. 1:15-cv-02671 (N.D. Ga., Mar. 16, 2017) (summary judgment for insurer under crime and computer fraud provisions when loss did not arise from use of a computer and when actions were not the direct causes of the alleged loss); Apache Corp. v. Great Am. Ins. Co., No. 15-20499 (5th Cir., Oct. 19, 2016) (reversing the lower court's summary judgment for the insured, the appellate court instead held for the insurer on the grounds that a fraudulent email that caused a misdirected funds transfer was "merely incidental to the occurrence of the authorized transfer of money.").

The stream of such cases flows on. For example, on April 7, 2017, a manufacturing policyholder moved for summary judgment in a case against its insurer. Seeking coverage under a computer crime policy, it contends that hackers got into both its own computer system and that of one of its parts suppliers, allowing apparently appropriate emails to be exchanged that resulted in three wire transfers to what turned out to be a fake account. The insurer has denied coverage because the loss was not directly caused by use of a computer and since the transfer did not come from inside the "premises" or from inside "financial institution premises" as defined by the policy. See *American Tooling Center, Inc. v. Travelers Cas. and Sur. Co. of Am.*, No. 16-12108 (E.D. Mich.).

And the litigation over losses from cyber-related risks also continues to involve much more traditional coverages, such as comprehensive general liability (CGL) policies. There have been several much-publicized cases in the past several years about whether harm to data constitutes "property damage," whether a hacker's access to or use of breached data is "publication" or creates "personal and advertising injury," and more. New filings involving such positions include, for example, *Charter Oak Fire Ins. Co. v. 21st Century Oncology Inv.*, LLC, No. 2:16-cv-00732 (M.D. Fla.) (motion to dismiss filed Jan. 17, 2017 over whether third party class actions following a patient data breach at the insured's oncology clinics concern a "publication" of data and a "personal injury"), *St. Paul Fire & Marine Ins. Co. v. Rosen Millennium, Inc.*, No. 6:17-cv-540 (M.D. Fla., filed Mar. 27, 2017) (new complaint seeking coverage for fines to credit card companies, investigative and notification costs, and other expenses associated with a data breach of customer payment cards), and *Yahoo! Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.*, No. 5:17-cv-00489 (N.D. Cal., filed Jan. 31, 2017) (complaint contending that email scanning suits pending against the insured allege "personal injury" or "personal and advertising injury").

The policy language, facts and jurisdiction will affect the outcomes in litigation or other proceedings. These recent filings illustrate that insureds and insurers present and face a wide array of arguments that will mark the legal landscape. Disputed claims will continue to shape the body of law that both insureds and insurers should consider in their insurance transactions going forward. And it rolls on.

Executive Orders Establish American Technology Council and Set Out Cybersecurity Initiatives

On May 1, 2017, President Trump signed the Presidential Executive Order on the Establishment of the American Technology Council (the ATC EO). The ATC EO is intended to "promote the secure, efficient, and economical use of information technology to achieve its missions" within the government of the United States through the establishment of the American Technology Council. Then, on May 11, 2017, President Trump signed the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (the Cybersecurity EO). Each of these EOs provides indications of the Trump administration's objectives with respect to technological developments and information security initiatives.

The Council created by the ATC EO is comprised of senior governmental officials, including the President and Vice President, who may preside over meetings of the Council; in their absence, the occupant of the newly-created position of Director of the American Technology Council will preside. The primary functions of the Council will include coordination of development of strategies for appropriate use of information technology by the United States Government, and advising the President with respect to the same. In furtherance of the goals of the Executive Order, the Director of National Intelligence (a member of the Council) is "encouraged to provide access to classified information on cybersecurity threats, vulnerabilities, and mitigation procedures to the [the Council] in order to facilitate the [Council]'s activities."

The Cybersecurity EO provides guidance and requirements for the cybersecurity of federal networks (largely through an accountability and risk management approach), critical infrastructure (including through assessment of risks and an initiative to improve internet resilience against botnets and other automated and distributed attacks), and promotion of cybersecurity measures for the nation, generally. The

provisions of the Cybersecurity EO relating to cybersecurity of the nation include assessments and reports relating to deterrence and protection options, international cooperation, and development of the cybersecurity workforce. This EO reflects a long-term view with respect to addressing cybersecurity concerns and may serve to guide development and deployment of cybersecurity measures and infrastructure going forward.

The promulgation of executive orders, and bodies within the Executive Branch relating to information technology issues, warrant the careful attention of any organization doing business with the federal government, and may eventually portend the setting of standards to be used by private organizations nationwide.

FCC Privacy Rules Repealed – Before Becoming Effective

On April 3, 2017, President Trump signed Senate Joint Resolution 34 (SJR 34), which effectively repealed not-yet-in-effect Federal Communications Commission regulations designed to limit use of customer information by broadband service providers and provide enhanced privacy protections for customers of those service providers. The FCC regulation, titled "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services" (81 Fed. Reg. 87274) had been promulgated during President Obama's Administration and would have imposed requirements on broadband providers with respect to treatment of customer data, including provision of privacy policies, customer consent for certain information collection and use practices, implementation of "reasonable" information security practices, and notification of information security breaches.

Opponents of SJR 34 generally see the repeal of the FCC's regulation as a major loss for consumer privacy – allowing for continued use of broadband customer information even in the absence of explicit consent, arguing, for example, that providers could sell browsing histories. (Notably, major providers Comcast, Verizon, and AT&T have indicated that they will not sell individual browsing histories.) The law's supporters note that the regulation would have imposed especially harsh requirements on broadband providers, as compared to relatively established, but comparatively relaxed rules in place for other online service providers, which have been established under the jurisdiction of the Federal Trade Commission and state laws.

Prior to the enactment of SJR 34, Federal Trade Commission Chairwoman Maureen K. Ohlhausen and Federal Communications Commission Chairman Ajit Pai issued a joint statement indicating a shared commitment to the protection of consumers' personal information and arguing that jurisdiction over the privacy and information security practices of broadband providers should be returned to the FTC, which had been the applicable regulator until 2015, as "the nation's expert agency with respect to these important subjects." Following passage of SJR 34, Chairman Pai issued another statement supporting the law and providing an assurance that "the American people to know that the FCC will work with the FTC to ensure that consumers' online privacy is protected though a consistent and comprehensive framework." These statements provide a strong indication that broadband providers should look to the regulatory actions and statements of the Federal Trade Commission to guide their decisions.

Some might speculate that SJR 34 may signal a more business-friendly approach to regulation in the privacy space during the Trump Administration. However, SJR 34 has generated considerable discussion in political and technological circles, and raises issues that will likely remain open for debate for the foreseeable future. Broadband providers, as well as other service providers would be wise to keep a careful eye on future actions and statements from the FTC with respect to treatment of consumer information.

FTC Releases Cross-Device Tracking Guidance

In January, the Federal Trade Commission (FTC) released guidance that will be of interest to companies that utilize cross-device tracking. Cross-device tracking refers to a company's ability to link a consumer's behavior on a website or an app to their behavior on a smartphone, tablet, television, laptop or other device. Simply put, cross-device tracking is the technology responsible for placing that vacation ad on your smartphone when you *only* researched vacations on your desktop browser.

The guidance warns that failure to disclose cross-device tracking activities to consumers could violate the FTC Act. Consistent with longstanding principles, the FTC recommends that a disclosure explains that cross-device tracking is being utilized, as well as what information is being collected, by what entities, and how it's used. For example, the guidance specifically cautions companies against stating they do not share "personal information" with third parties if they provide usernames or email addresses (raw or hashed) to cross-device tracking companies.

Additionally, the guidance recommends providing choices on how consumer activity is tracked across devices, including opt-out tools. While the guidance stops short of requiring opt-out tools, companies that provide opt-out tools should clearly disclose their existence, along with any limitations on how they apply. For example, if a company's existing opt-out tools do not apply to cross-device tracking, that should be disclosed.

Finally, the guidance recommends coordination between third-party cross-device tracking companies and first-party, consumer-facing companies. In other words, third-party companies should make the same type of disclosures that a first-party company would make to a consumer.

The bottom line for companies is this: any company that utilizes cross-device tracking should review and revise its privacy policy to ensure that its practices, along with any related choices provided to consumers, are appropriately disclosed.

A New Member in the Big Club – New Mexico Becomes the 48th State with a Breach Notification Law (+ Disposal and Service Provider Requirements)

Effective June 16, 2017, New Mexico will join 47 other states (as well as the District of Columbia, Guam, Puerto Rico, and the Virgin Islands) by imposing breach notification requirements on entities experiencing information security breaches impacting the state's residents. Recently-passed House Bill 15 will impose

significant new requirements on businesses in New Mexico, and add new considerations for any businesses dealing with New Mexico residents when responding to an incident.

The new law is largely in line with the laws of other states, requiring notification following the unauthorized acquisition of unencrypted personal data, or encrypted personal data along with a process or key to decrypt the data. Certain elements of the law that are not common among all states are particularly noteworthy when responding to an incident:

- notifications generally must be provided in the most expedient time possible and not more than 45 days following discovery of a breach;
- biometric data is included in the definition of personal information types that (along with name) can trigger a breach notification requirement;
- specific requirements are imposed for the content of notifications (including, without limitation, disclosure of data types subject to the incident, date or estimated date of the incident, a description of the incident, contact information for the entity experiencing the incident, toll free numbers for the major consumer reporting agencies, advice to review account statements and credit reports, and advice informing recipients of their rights under the federal Fair Credit Reporting Act); and
- the major consumer reporting agencies and the state's attorney general must be notified if notices are provided to more than 1,000 New Mexico residents in connection with one incident.

In addition to imposing breach notification requirements, HB 15 imposes several basic information security requirements, including:

- implementation and maintenance of reasonable security procedures and practices appropriate to the nature of the information to protect the personal identifying information from unauthorized access, destruction, use, modification or disclosure;
- contractual provisions requiring service providers to maintain appropriate procedures and practices to protect personal information disclosed in the course of a service provider engagement; and
- proper disposal of personal identifying information when no longer reasonably needed for a business purpose. ("Proper disposal" is defined as "shredding, erasing or otherwise modifying the personal identifying information contained in the records to make the personal identifying information unreadable or undecipherable.")

Following the passage of HB 15, organizations in New Mexico or dealing with information relating to New Mexico residents should be aware of the state's new data breach requirements to ensure that responses are handled appropriately, and in a timely manner. Those organizations should also review day-to-day practices to make sure that appropriate disposal and service-provider-engagement practices are in place.

HIPAA Enforcement Update (February 2017 – April 2017)

In recent months, the Department of Health and Human Services, Office for Civil Rights (OCR) has announced four settlement agreements and one civil monetary penalty to resolve allegations of Health Insurance Portability and Accountability Act (HIPAA) violations. Four of the enforcement actions signal OCR's focus on the HIPAA Security Rule, particularly the need for organizations to audit and assess risks to electronic protected health information (ePHI) and to implement corrective action when security risks are identified. In addition, OCR again stresses the need for entities subject to HIPAA to enter into a business associate agreement (BAA) with downstream organizations receiving patients' protected health information (PHI), the importance of adopting comprehensive HIPAA policies and procedures, and maintaining strong processes relating to access controls.

Most recently, on April 24, 2017, OCR announced a $2.5 million settlement agreement with CardioNet, an organization that provides remote mobile monitoring of and rapid response to patients at risk for cardiac arrhythmias. CardioNet filed a data breach report with OCR when a workforce member's laptop, containing ePHI of 1,391 individuals, was stolen. OCR's subsequent investigation revealed CardioNet had insufficient risk analysis and risk management processes as required by the HIPAA Security Rule. Furthermore, CardioNet's data security policies and procedures were still in draft form and had not yet been implemented. When announcing this settlement, OCR noted that mobile devices remain particularly vulnerable for potential data breaches and the settlement signals that an organization's failure to implement appropriate security safeguards for these devices may incur penalties.

On April 20, 2017, OCR issued a press release indicating that the Center for Children's Digestive Health ("CCDH") paid $31,000 to settle potential HIPAA violations for its failure to enter into a BAA with a downstream contractor, FileFax, Inc. (FileFax). In August 2015, OCR initiated an investigation of FileFax, a company that stored records containing PHI for CCDH. OCR found that although CCDH began disclosing PHI to FileFax in 2003, neither CCDH nor FileFax could produce a signed BAA dated prior to October 12, 2015. This settlement highlights the importance of obtaining BAAs with all vendors prior to disclosing PHI and signals that, although business associates are now directly liable for compliance with certain aspects of HIPAA, BAAs remain an important component of HIPAA compliance.

On April 12, 2017, Metro Community Provider Network (MCPN) agreed to a $400,000 settlement with OCR for its lack of security management process to safeguard ePHI. The settlement arises from a breach report MCPN filed with OCR disclosing a phishing incident in which a hacker accessed MCPN employees' e-mail accounts and obtained the ePHI of 3,200 individuals. OCR's investigation revealed that prior to the incident, MCPN failed to conduct a risk analysis as required by the HIPAA Security Rule to assess the risks and vulnerabilities with respect to its ePHI. Furthermore, OCR concluded that the risk analysis conducted after the phishing incident and subsequent analyses were insufficient to meet the requirements of the Security Rule. When determining the $400,000 settlement amount, OCR considered MCPN's status as a federally-qualified health center and balanced the significance of the violation with MCPN's ability to maintain sufficient financial standing to ensure the provision of its ongoing

patient care. OCR has released a significant amount of guidance on Security Rule compliance and risk analysis. In July 2016, OCR released a Fact Sheet on healthcare ransomware attacks.

On February 16, 2017, OCR issued a press release announcing a $5.5 million settlement with Memorial Healthcare System (MHS) in relation to MHS's inaction allowing unauthorized users to access ePHI of 115,143 individuals through use of login credentials belonging to a former employee of a physician practice affiliated with MHS through an Organized Health Care Arrangement (OHCA). According to the press release, although MHS had workforce access policies and procedures in place, MHS failed to implement procedures with respect to reviewing, modifying and/or terminating users' right of access. Further, OCR found that MHS failed to regularly review records of information system activity on applications that maintain ePHI by workforce users and users at affiliated physician practices, despite having identified this risk on several risk analyses conducted by MHS from 2007 to 2012. Following announcement of this settlement, Robinsue Fohboese, OCR's Acting Director, stated that "organizations must implement audit controls and review audit logs regularly. As this case shows, a lack of access controls and regular review of audit logs helps hackers or malevolent insiders to cover their electronic tracks, making it difficult for covered entities and business associates to not only recover from breaches, but to prevent them before they happen."

Lastly, on February 1, 2017, OCR announced a $3.2 million civil money penalty against Children's Medical Center of Dallas (Children's) predicated on Children's impermissible disclosure of unsecured ePHI and prolonged non-compliance with multiple HIPAA Security Rule standards. Children's first filed a breach report with OCR in 2010 when a non-password-protected mobile device containing ePHI of approximately 3,800 individuals was compromised. Three years later, in 2013, Children's filed another breach report when an unencrypted laptop containing the ePHI of approximately 2,462 individuals was stolen from its premises. OCR's investigation revealed that in 2007 and 2008 Children's had received external recommendations relating to laptop encryption through security risk assessments and gap analyses that identified the lack of risk management as a high risk issue. Accordingly, OCR concluded that, despite Children's awareness of the risks involved with maintaining unencrypted ePHI on mobile devices, it continued to allow its workforce to utilize unencrypted devices until after its second data breach incident in 2013. Although OCR prefers to settle cases and assist entities in implementing corrective action plans, circumstances in this case led OCR to pursue full civil monetary penalties against Children's and issuance of a Final Notice of Determination.