Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 33, ISSUE 12 / NOVEMBER 20, 2015

WHAT'S INSIDE

CYBERSQUATTING

Olympics organizers say cybersquatter is blocking website for 2020 games

By Patrick H.J. Hughes, Managing Editor, Westlaw Daily Briefing

The International Olympic Committee and its U.S. counterpart say in a complaint filed in Houston federal court that a cybersquatter is preventing them from registering an official domain name for the 2020 Olympic Games in Tokyo.

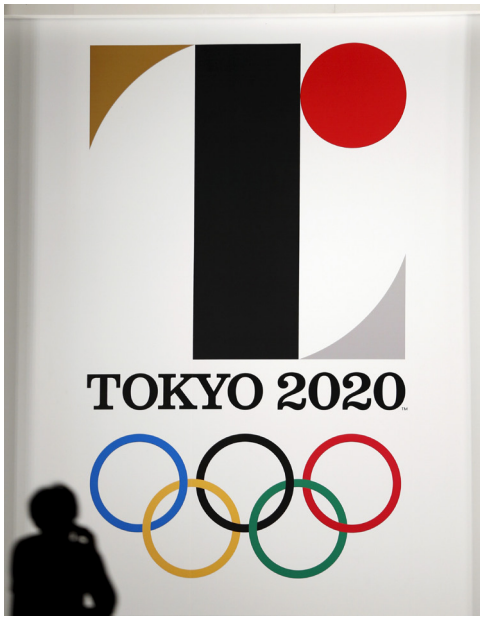
International Olympic Committee et al. v. Frayne et al., No. 15-cv-3277, complaint filed (S.D. Tex., Houston Div. Nov. 5, 2015).

Stephen P. Frayne Jr. had already registered the domain Tokyo2020.com, and he did so for an illegitimate purpose, the suit filed in the U.S. District Court for the Southern District of Texas says.

The IOC and the U.S. Olympic Committee claim that Frayne and his company CityPure LLC have "speculatively register[ed] and stockpil[ed] hundreds of domain names consisting of Olympic city-year names ... many years in advance of the Olympic Games and cybersquatt[ed] upon them in the hope that they will match valuable Olympic bid or host cities."

The complaint follows a 2008 dispute between the USOC and Frayne over the domain chicago2016.com that ended in a settlement

CONTINUED ON PAGE 20



REUTERS/Issei Kato

The international and U.S. Olympic committees say Stephen P. Frayne Jr. is unlawfully seeking to profit from another's trademarks by registering, with future dates, domains with the names of cities that have previously hosted the games, such as such as "Tokyo 2020," shown on this Olympic emblem in Tokyo earlier this year.

COMMENTARY

Financial institutions' proactive steps to data breach recovery

Richard Milam of EnableSoft discusses the steps financial institutions can take to safeguard customer accounts when credit and debit card information is compromised by hackers.

SEE PAGE 3

41737780

Westlaw Journal Computer & Internet

Published since November 1983

Publisher: Mary Ellen Fox

Managing Editor: Robert W. McSherry

Editor: Melissa Sachs, Esq.
Melissa.Sachs@thomsonreuters.com

Managing Desk Editor: Robert W. McSherry

Senior Desk Editor: Jennifer McCreary

Desk Editor: Sydney Pendleton

Graphic Designers: Nancy A. Dubin
Ramona Hunter

Thomson Reuters
175 Strafford Avenue, Suite 140
Wayne, PA 19087
877-595-0449
Fax: 800-220-1640
www.westlaw.com
Customer service: 800-328-4880

For more information, or to subscribe, please call 800-328-9352 or visit west.thomson.com.

For the latest news from Westlaw Journals, visit our blog at http://blog.thomsonreuters.com/westlawjournals.

How to Find Documents on Westlaw
The Westlaw number of any opinion or trial filing is listed at the bottom of each article available. The numbers are configured like this: 2015 WL 000000. Sign in to Westlaw and on the "Welcome to Westlaw" page, type the Westlaw number into the box at the top left that says "Find this document by citation" and click on "Go."

Westlaw

TABLE OF CONTENTS

Financial institutions' proactive steps to data breach recovery

By Richard Milam
EnableSoft

If Donald Trump's hotel chain can be breached by hackers, no consumer is safe from credit and debit card fraud. In addition, big box retailers offer little reassurance that consumers are safe to shop at their stores. In fact, fraudsters had more than a year — from May 19, 2014, to June 2 of this year — to steal Trump's hotel customers' card numbers, expiration dates and security codes.

The Trump Hotel Collection was quick to notify the FBI, an outside forensic expert and financial institutions of the potential data breach. The fraudulent card transactions that occurred at Trump hotels, however, spurred banks to alert the company of the possible breach in June.

The company released this statement: "Like virtually every other company these days, we have been alerted to potential suspicious credit card activity and are in the midst of a thorough investigation to determine whether it involves any of our properties."[1]

The data breach occurred at seven Trump hotels. While independent forensic investigators have not found instances where customers' information has been misused, this does little to ease the minds of those who may have stayed at one of the hotels during the year when the payment systems were hacked.

Trump's hotel customers are not the only ones concerned for their personal information security. In fact, all consumers risk having their personal identification and financial information infiltrated by fraudsters whenever they swipe a credit or debit card.

CARD FRAUD IS PREVALENT

Credit and debit card fraud is one of the top causes of identity theft in the United States. The U.S. Department of Justice reported an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014. Of those victims, 86 percent experienced the fraudulent use of existing account data, such as credit card or bank account information.[2]

Data breaches are now one of the top concerns of businesses throughout the United States. This concern has spurred the movement to EMV cards — Europay, MasterCard and Visa — which are credit and debit cards installed with microchip technology that is used to authenticate transactions. The new chip-and-signature and chip-and-pin methods offer a more secure method of payment for consumers. The new methods, however, force financial institutions and retailers to add new in-store technologies and payment processing systems.

All consumers are at a risk of having their personal identification and financial information infiltrated by fraudsters whenever they swipe a credit or debit card at any retailer or merchant.

WHO SHOULDERS THE BLAME FOR DATA BREACHES?

Under the federal Truth in Lending Act, 15 U.S.C. § 1643, cardholders are essentially not liable for financial damage stemming from fraudulent charges. And with the movement to EMV cards there is a "liability shift," with the blame now on the party that has lesser technology in the event of a data breach.

Customer service and security are high priorities for banks and credit unions, which have been rushing to issue chip cards for all account holders. It appears from the Trump hotel chain incident that retailers and merchants are not acting as quickly to install chip credit card readers in their stores or at their point-of-sale locations. This means data theft will still occur.

Financial institutions have little authority over what retailers and merchants do at their point-of-sale locations. They do, however, have the power to buffer whatever effects customers experience after a seemingly inevitable — yet unpredictable — data breach.

TECHNOLOGY TOOLS

As they compete to deliver top customer service, security and protection, banks and credit unions across the United States are quickly delivering chip cards to their customers through the power of in-house automation tools. This allows them to beat the clock by delivering the new cards before retailers and merchants have installed chip credit card readers.

Having a chip card does little to prevent a data breach at merchant locations that do not have EMV-compatible technology. However, the technology that is used to issue EMV cards on a mass basis also enables banks and credit unions to quickly react when disaster strikes. Thus, they can help mitigate the exposure, loss and inconvenience that their customers experience.

By using robotic process automation technology, financial institutions are able to quickly identify which accounts have been

Richard Milam, an early innovator in the robotic process automation market, in 1995 founded Orlando, Fla.-based **EnableSoft**, which creates the Foxtrot automation technology software. He serves as company CEO and can be reached at rmilam@enablesoft.com.

breached and proceed with the data recovery process. This minimizes service downtime and preserves customer relationships.

What is robotic process automation? Simply put, it is training a computer — or virtual robot — to perform a data task or process through a series of scripts. Scripts are the step-by-step actions that one would teach a human who was learning to perform the process manually. The saved script, or set of instructions, can then be used repeatedly to perform the data process.

Compared to humans, robots perform data processes much more quickly and precisely. They can also be trained to execute an infinite number of data processes, which is of value for banks that run multiple, recurring data jobs on a daily, monthly and yearly basis.

Banks, credit unions, card issuers and even retailers that are prepared for data breaches have adopted robotic process automation in their organizations to not only reduce their risk of a devastating data breach but also to perform many routine data-related tasks and processes.

Here are five common steps that nearly 500 bank and credit union customers took to better protect cardholders and mitigate the effects of a data breach.

STEP 1: QUERY ACCOUNTS FOR FRAUD

Generally, after learning of a suspected breach, financial institutions are forced to wait for a "compromised account management system" alert regarding fraudulent account activity. A CAMS alert is the private notice financial institutions receive from card associations, such as Visa and MasterCard, containing a list of the accounts that may have been affected. Once aware of the compromised accounts, banks proceed with additional recovery steps and reissue the credit or debit cards.

Unfortunately, the time between the data breach and CAMS delivery to the bank is often too slow to be impactful. In fact, it can take upward of weeks for banks to learn which customer accounts may have been affected.

After a breach is identified, however, proactive financial institutions use automation to scan their customer accounts for transactions at the compromised retailer(s) during the time period in question, and flag them.

The safest course of action once a transaction is flagged is to cancel the credit or debit card and issue a new one promptly. Customers who may have been impacted by the data breach experience a quick response and little downtime with respect to their finances and security.

Furthermore, only flagged customers receive a new card; the bank does not have to issue new cards to all cardholders.

STEP 2: ADJUST ACCOUNT SPENDING LIMITS

We live in a cashless society. Many consumers cannot afford to live without being able to use their credit or debit card as a payment method. If it is not feasible to cancel a card immediately, which is most often the case, banks can still mitigate risk by reducing customers' spending limits. This technique allows customers to continue to use their cards until they receive new ones.

> Credit and debit card fraud is one of the top causes of identity theft in the United States.

When Massachusetts-based StonehamBank learned they had as many as 900 cards compromised in 2013's Target stores data breach, it reduced PIN purchase transaction limits from $3,500 to $1,500 and set signature transaction limits to $0. These actions allowed cardholders to make relatively secure transactions while protecting them, and the bank, from loss.

STEP 3: CREATE 'HOT CARD' PROCEDURE

Having a plan in action to place a "hot card" designation on compromised cardholders' accounts is half the battle, and a big one at that. Most core banking systems enable users to add designations to accounts, but adding a "hot card" status manually to hundreds or thousands of accounts can be an onerous, inefficient task that prolongs customer service and opens the door for numerous errors and invalid data.

The use of robotic process automation to search, flag and cancel compromised card accounts saves an enormous number of employee man-hours and eliminates the risk of human error.

It would be upsetting, and an example of poor customer service, for a cardholder to receive a new card and find out that it does not authorize payment because an employee mistyped a digit in the account number. The manual effort needed to search and flag compromised accounts drains resources, leads to poor customer service and risks an institution's data integrity. Robotic process automation empowers banks to recover their customers' spending freedom efficiently and accurately.

STEP 4: ISSUE NEW CARDS

For all involved (retailers, payment processors, card issuers and cardholders), the ultimate and universal goals following a data breach are to mitigate customers' risk of further exposure to theft and to get a new card into their hands as soon as possible.

A bank's preemptive card reissue plan must include strategies on how to issue new cards to customers at different levels of compromise. For example, reissuing one card manually is not as daunting as reissuing 1,000 cards manually. Robotic process automation makes card reissuance the fastest, easiest and most accurate process because the same script can be opened and run at any time and for any number of cards. Mass card reissues will undergo the same actions as a single card reissue.

Automating the card reissuance process undoubtedly allows banks to reach the ultimate goals following a data breach. They will be able to provide their cardholders with the best customer service, minimal downtime and increased risk mitigation. Robotic process automation technology makes these things possible.

STEP 5: NOTIFY CUSTOMERS

It can take weeks for financial institutions to confirm which of their cardholders are at risk in the aftermath of a data breach. That said, they are not the only parties that need to be notified in the event of a breach. Unfortunately, it is the customer — the victim of the crime — who is often the last to find out.

Before automation tools hastened the notification process, the act of alerting customers about a potential risk took the form of a letter in the mail, which prolonged delivery of the news even further.

Proactive banks keep customers informed during each step of the data breach recovery

process. They send customers emails and letter notifications, and they post memos to customer accounts. Maintaining a clear line of communication with customers eases the fears arising from the news of card fraud and reassures them that their bank is working toward a resolution.

Banks have discovered that automating these breach recovery processes frees up staff, such as in the call center, further boosting their provision of customer service. Call center representatives are not burdened with the tasks of adding addendums to accounts while trying to answer cardholders' calls and questions.

Although retailers shoulder much of the blame for large data thefts, banks often receive unwarranted scorn from customers who believe they should have been better protected.

A bank that is able to initiate contact with a customer about a breach, and even reissue cards before the news goes public, can virtually eliminate any ill will or bad press that might occur as a result.

As financial institutions move to more omnipresent environments, proactive banks should consider how resources will be allocated and who will accomplish tasks when developing a data breach recovery plan. Formerly, in the wake of data theft, a bank's only option was to pull staff from often-critical areas or bring in and pay a team over one or more weekends to stumble through the recovery process.

Some institutions may still turn to their core system provider or another third-party vendor for some support. But since these entities' priorities lie in operating the main business functions, such solutions often do not address all of the functionality needed to fully support the data breach recovery process.

CONCLUSION

Fortunately, today's proactive banks are empowered with automation technology to perform the data breach recovery processes for them. A plan of action, a fully focused staff and the right automation tools enable banks to recovery quickly, safely and effectively following a data breach. WJ

NOTES

[1] Brian Krebs, *Banks: Card Breach at Trump Hotel Properties,* KrebsOnSecurity (July 1, 2015), *available at* krebsonsecurity.com/2015/07/banks-card-breach-at-trump-hotel-properties/

[2] Erika Harrell, Bureau of Justice Statistics, Pub. No. NCJ 248991, Victims Of Identity Theft, 2014 (2015), http://1.usa.gov/1LeeTmg.

U.S. justices divided over class action suit against Spokeo

(Reuters) – The U.S. Supreme Court on Nov. 2 appeared closely divided as it considered online people-search service Spokeo Inc.'s bid to avoid a class-action lawsuit for including incorrect information in its database.

Spokeo Inc. v. Robins, No. 13-1339, oral argument held (U.S. Nov. 2, 2015).

The legal issue before the nine justices was whether a plaintiff can sue for a technical violation of a federal consumer law even when there is a question about whether the person has been directly harmed. Some of the court's conservatives appeared hostile to the plaintiff's claims, but the liberal justices pushed back against Spokeo.

The case gives the conservative-leaning Supreme Court another shot at limiting class-action litigation as it has done in a series of decisions including a 2011 victory for Wal-Mart Stores Inc. *Wal-Mart Stores v. Dukes*, 131 S. Ct. 2541 (2011).

But Justice Anthony M. Kennedy, who often casts the deciding vote in close cases, was less outspoken than several of his conservative colleagues, giving little indication as to how he would vote.

In 2010 plaintiff Thomas Robins filed suit in California on behalf of himself and other people potentially harmed by incorrect information about them that Spokeo might disseminate.

The suit was filed under the federal Fair Credit Reporting Act, 15 U.S.C. § 1681, which requires consumer reporting agencies to provide correct information. Spokeo, which says it is not a consumer reporting agency, is seeking to have the lawsuit thrown out.

Robins' lawsuit was filed two years before Spokeo agreed to pay $800,000 to settle U.S. Federal Trade Commission claims that it had violated the Fair Credit Reporting Act when attempting to sell data to other companies.

Robins, who is unemployed, asserted that his Spokeo entry had damaged his job-seeking prospects because it contained inaccurate information. The entry, for example, stated Robins has a graduate degree, which he said is incorrect.

Chief Justice John G. Roberts Jr. was among the conservative members of the court who appeared sympathetic to Spokeo.

"We have a legion of cases that say you have to have actual injury" in order to sue, Chief Justice Roberts said.

Liberal Justice Elena Kagan contested Spokeo's assumption that Robins was not harmed. Justice Kagan said Robins' claim "seems like a concrete injury to me" and that if a company distributed incorrect information about her, "I would feel harmed."

A ruling is due by the end of June.

Facebook, Google and Yahoo have all faced similar lawsuits over violations of different federal laws. As many online companies have millions of users, a case can quickly become a multimillion-dollar class action. WJ

(*Reporting by Lawrence Hurley; editing by Will Dunham*)

> Some of the high court's conservatives appeared hostile to the plaintiff's claims, but the liberal justices pushed back against defendant Spokeo Inc.

Attorneys:
Petitioner: Andrew J. Pincus, Mayer Brown, Washington

Respondent: William S. Consovoy, Consovoy McCarthy Park PLLC, Arlington, Va.

Amicus curiae (United States): Deputy Solicitor General Malcolm L. Stewart, Justice Department, Washington

Related Court Document:
Oral argument transcript: 2015 WL 6673854

Spokeo v. Robins: Experts comment on constitutional standing

By Melissa J. Sachs, Esq., Senior Legal Writer, Westlaw Journals

Practitioners at law firms across the country discuss what's at stake in a case pending before the U.S. Supreme Court against Spokeo Inc., which purportedly runs a website that collects and publishes consumer "credit estimates."

The issue before the nation's high court is whether Thomas Robins has constitutional standing to bring his proposed federal class action, which alleges Spokeo willfully violated the Fair Credit Reporting Act.

According to Robins' lawsuit, Spokeo failed to maintain accurate records and falsely published information indicating he is wealthy and holds a graduate degree.

Robins, who is unemployed, says Spokeo's false report lowered his potential employment prospects.

Article III of the U.S. Constitution limits the federal judiciary's power to resolving only live "cases" and "controversies."

The Supreme Court has interpreted in *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992), this to mean plaintiffs must have suffered an "injury-in-fact" to have standing to sue in federal court.

To meet the injury-in-fact requirement, plaintiffs like Robins must show actual or imminent, concrete and particularized injuries.

This case asks whether Spokeo's alleged willful violation of the FCRA is a sufficient injury to show standing or whether Robins and other plaintiffs must allege actual harm beyond the website's alleged statutory violations.

Westlaw Journals asked legal practitioners what this case means for future class actions and federal court standing.

Mary-Christine "M.C." Sungaila, Haynes & Boone

Spokeo raises an issue that strikes at the heart of the Constitution's division of powers between the legislature and the judiciary: Can Congress create a cause of action in a statute that will satisfy the constitutional requirement for actual injury or must there be additional evidence of actual harm to satisfy the requirements of Article III?

The answer will have enormous practical importance because there are many federal causes of action that raise this issue and that could open the door to lawsuits, including potentially large and costly multimillion-dollar class actions.

As the U.S. Chamber of Commerce and International Association of Defense Counsel pointed out in our *amici* brief in support of Spokeo, these statutes include the Fair Credit Reporting Act [15 U.S.C. § 1681], the Telephone Consumer Protection Act [47 U.S.C. § 227], and other privacy-oriented federal statutes.

At oral argument, Justice [Anthony M.] Kennedy asked Spokeo's counsel whether there might be some way to draft FCRA that might allow Robins to bring a suit. Spokeo's counsel answered that there might be if Congress were to make clear it was singling out these kinds of injuries as inflicting a certain kind of harm, but that because Congress had not done so in the statute, Robins lacked standing.

This suggests a possible approach to amending the statute to comply with Article III, but it would still require threading the needle between congressional power and the limits placed on it by the Constitution and the courts.

Douglas G. Smith, Kirkland & Ellis

The injury-in-fact requirement is important in its own right, but its importance is magnified where, as in the Spokeo case, plaintiffs are seeking to represent a class of potentially thousands of plaintiffs without any demonstrable concrete injury.

Even those members of the court who suggested during argument that the injury-in-fact requirement may be satisfied with respect to the named plaintiff seemed somewhat skeptical of a broader ruling that *all* potential members of the class were injured based solely on an alleged violation of a federal statute.

Accordingly, regardless of the outcome, the decision in *Spokeo* may present significant hurdles for plaintiffs seeking to pursue similar class actions in the future.

Anthony "Tony" T. Lathrop, Moore & Van Allen

Spokeo raises a "hot button" issue, given the rise of data breach, Fair Credit Reporting Act and other class actions based on companies' violations of statutory requirements that do not necessarily result in actual damages to the plaintiffs.

Oral arguments revealed a division of the Supreme Court, with several justices seeming to lean toward a narrow finding that Congress has authority to create a cause of action under the FCRA for individuals about whom false information was reported, on the grounds that the dissemination of false information by a credit reporting agency is itself injury-in-fact sufficient to give rise to Article III standing. Other justices, however, raised several concerns with that view given the FCRA does not require publication of false information for an individual to sue a company that has violated the statute's procedures, and hypotheticals they posited illustrated that publication of false information about an individual may not cause any actual harm. Justice [Sonia] Sotomayor clearly stated that she believes that "the breach of any legal right you're given ... gives Article III jurisdiction," but where the court ultimately will come out on the question presented remains to be seen.

If plaintiffs must prove injury-in-fact beyond allowable statutory damages, defendant companies will have another weapon in their arsenal to limit class actions before costly settlement or protracted litigation.

Michael R. Pennington, Bradley Arant Boult Cummings

I think the questions from the justices in oral argument suggest that the specific facts of *Spokeo* may not present the real issue as cleanly as another case might have.

For example, numerous federal statutes applicable to lenders and mortgage servicers, such as the Fair Debt Collection Practices Act [15 U.S.C. § 1692], require notices containing certain information to be sent within a certain number of days of a given event. If the notice is sent a day late, then even if the notice was otherwise perfectly accurate and even if the customer already new all of the information, some courts say the lender or mortgage servicer is automatically liable for statutory damages, potentially on a class-wide basis.

If Congress can make that scenario privately actionable, then Congress effectively has the power to circumvent Article III's "actual injury" requirement at will, without the need for a constitutional amendment.

Some justices seemed to feel that Congress needs to have the power to create procedures designed to ensure accuracy and demand strict compliance with them.

That line of questioning misses the point. Congress does have that power.

It's the job of the executive branch to enforce laws designed to ensure that prophylactic procedures are followed even if their violation produces no actual harm. The executive branch can and does fine, cite, enjoin, revoke licenses and so on when such procedures are not followed, even if the violation produces no actual harm.

But the desire to ensure compliance with prophylactic procedures is not a reason to look the other way on the absence of actual harm when it comes to private lawsuits. To sanction that gives Congress a power it does not have under the Constitution — the power to define the absence of injury as injury, and thereby nullify a major part of Article III. WJ

Privacy suit over Google's Internet tracking continues

By Melissa J. Sachs, Esq., Senior Legal Writer, Westlaw Journals

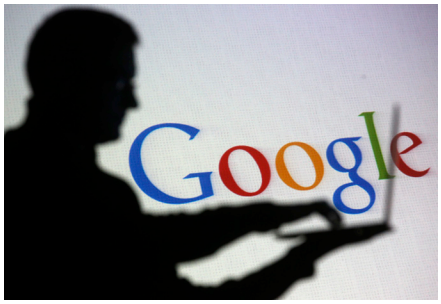
A federal appeals court has revived part of a consumer class action alleging Google secretly placed small files on users' personal computers to track their online habits, circumventing privacy settings on Safari and Internet Explorer browsers.

In Google Inc. Cookie Placement Consumer Privacy Litigation, No. 13-4300, 2015 WL 6875340 (3d Cir. Nov. 10, 2015).

The consumers in the proposed class action may continue with their claims that Google violated California's constitution and state tort laws, the 3rd U.S. Circuit Court of Appeals' opinion said.

"Based on the pled facts, a reasonable fact finder could indeed deem Google's conduct 'highly offensive' or 'an egregious breach of social norms,'" Judge Julio M. Fuentes wrote for the three-judge appellate panel.

The appeals court rejected Google's arguments that "cookies," the small files that the search giant allegedly placed on users' computers to track their online browsing behavior, are innocuous or routine.



REUTERS/Dado Ruvic

> "Based on the pled facts, a reasonable fact finder could indeed deem Google's conduct 'highly offensive' or 'an egregious breach of social norms,'" the 3rd Circuit said.

Instead the panel focused on the consumers' allegations regarding Google's public promises to respect users' privacy settings, including cookie blockers on Safari and Internet Explorer browsers, and the search giant's ultimate "deceit and disregard."

"What is notable about this case is *how* Google accomplished its tracking," Judge Fuentes wrote.

The panel reversed the U.S. District Court for the District of Delaware's decision to dismiss the two California privacy claims.

The appeals court, however, upheld the lower court's decision to dismiss the consumers' claims under the Wiretap Act, 18 U.S.C. § 2510; the Stored Communications Act, 18 U.S.C. § 2701; and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

The appellate panel also affirmed the dismissal of the consumers' other state law claims, including those alleging Google violated California's Invasion of Privacy Act, Cal. Penal Code § 630, and unfair-competition statute, Cal. Bus. & Prof. Code § 17200.

According to the consumers' lawsuit, Google serves third-party advertisements on websites and uses third-party cookies, or small files installed on users' computers, to track their Internet browsing habits.

Certain Web browsers such as Safari and Internet Explorer offered cookie-blockers to give users the choice to accept or block these files, the suit said.

Google publicly announced that it respected these cookie-blockers, the suit said. The proposed plaintiffs allegedly used these cookie-blockers, but Google developed a work-around and secretly placed cookies on their computers, they said.

In 2012 a Stanford graduate student revealed Google's covert work-around, according to the 3rd Circuit's opinion.

Consumers filed several lawsuits against Google, which were consolidated in the Delaware federal court, the district where the search giant is incorporated.

The Justice Department also sued Google, which eventually agreed to pay a $22.5 million penalty to resolve the suit through a stipulated order, but admitted no wrongdoing (see *Westlaw Journal Computer & Internet,* Vol. 30, Iss. 14, 30 No. 14 WJCOMPI 4).

In 2013 Google similarly settled claims with 37 states and the District of Columbia for $17 million (see *Westlaw Journal Computer & Internet,* Vol. 31, Iss. 13, 31 No. 13 WJCOMPI 12).

The Delaware federal court dismissed the consumers' consolidated lawsuit, finding they failed to state claims for relief.

The plaintiffs appealed, but the 3rd Circuit upheld most of the lower court's findings.

It reversed, however, on the California constitutional and state tort claims, which it remanded for further proceedings. WJ

Attorneys:
Plaintiff-appellants: Jason O. Barnes, Barnes & Associates, Jefferson City, Mo.; Edward D. Robertson Jr., Bartimus Frickleton Robertson & Gorny, Jefferson City; James P. Frickleton, Bartimus Frickleton Robertson & Gorny, Leawood, Kan.; Brian R. Strange, Strange & Butler, Los Angeles

Defendant-appellee: Colleen Bal and Michael H. Rubin, Wilson, Sonsini, Goodrich & Rosati, San Francisco; Anthony J. Weibell, Wilson, Sonsini, Goodrich & Rosati, Palo Alto, Calif.

Related Court Document:
Opinion: 2015 WL 6875340

Justices hear arguments in first of 3 cases that could transform consumer class actions

By Michael Scott Leonard, Senior Legal Writer, Westlaw Journals

At oral argument in the first of three U.S. Supreme Court cases that could transform consumer class actions this term, the justices signaled that the outcome may turn more on practical concerns than on the jurisdictional technicalities the plaintiff's lawyers sought to emphasize.

Campbell-Ewald Co. v. Gomez, No. 14-857, oral argument held (U.S. Oct. 14, 2015).

Throughout the Oct. 14 hearing, the justices pressed Stanford law professor Jonathan F. Mitchell — who is representing Jose Gomez, the consumer seeking the right to lead a class action against advertising giant Campbell-Ewald Co. — about the esoteric legal distinctions Gomez has made central to his case.

Gomez, who is suing Campbell-Ewald over unsolicited mass text messages it allegedly sent out on a client's behalf, has argued that the advertiser did not render moot his claims under the Telephone Consumer Protection Act, 47 U.S.C. § 227, when it offered to settle with him before class certification for the maximum amount he could legally recover.

Campbell-Ewald, meanwhile, says that even if there is a potential plaintiff class out there that could sue the company under the TCPA, Gomez no longer has standing to lead the suit.

Having rejected an offer of complete relief, he is no longer party to the sort of live "case or controversy" that is a jurisdictional prerequisite under Article III of the U.S. Constitution, the advertiser has argued.

The 9th U.S. Circuit Court of Appeals sided with Gomez last year, saying a ruling in the company's favor would effectively allow any defendant to head off a class action altogether by picking off named plaintiffs one at a time, before class certification, with settlement offers that leave them suddenly unfit to lead the case. *Gomez v. Campbell-Ewald Co.*, 768 F.3d 871 (9th Cir. 2014).

During argument Oct. 14, Mitchell told the justices repeatedly that a rejected settlement offer cannot itself moot a case under any circumstances. Mootness is a jurisdictional question, he said, and an unaccepted settlement offer is a defense on the merits.

"[I]f the defendant throws up his hands and unconditionally surrenders, whether it's a class action or not, that has nothing to do with mootness," Mitchell said. "It may justify a forced entry of judgment, but it does not moot the case."

The argument seemed to meet skepticism from justices at both ends of the court's ideological spectrum.

While questioning Mitchell, Justice Anthony Kennedy presented a hypothetical situation, asking what kind of case or controversy would remain if one person sued another for $10,000, the defendant offered to hand over the full $10,000, and the plaintiff rejected the offer.

REUTERS/Gary Cameron

"You won't take yes for an answer," Chief Justice John Roberts told the plaintiff's lawyer at one point.

"What is the concrete injury ... that results in adversity?" he asked.

In that case, Mitchell said, the defendant can — and should — win the case on the merits by raising the rejected offer as an affirmative defense under a theory like waiver, estoppel, failure to mitigate damages or accord and satisfaction.

But the court must still make that finding on the merits rather than tossing the case at the outset for mootness, which is a type of dismissal for lack of jurisdiction, Mitchell argued.

"Everyone agrees, Justice Kennedy, that under your hypothetical, the case should be thrown out of court," he said. "The only dispute is whether it's thrown out of court on jurisdictional grounds under Article III or whether it's bounced on the merits because the defendant has an affirmative defense.

'WHO CARES?'

According to Mitchell, the distinction between a jurisdictional dismissal and a dismissal on the merits is critical to the case because of the order in which trial judges analyze mootness, class certification and merits defenses.

If a plaintiff whose claims are moot files a class-action complaint, the judge should toss the suit for lack of jurisdiction before deciding whether to certify a plaintiff class, Mitchell noted. That is the outcome Campbell-Ewald is seeking.

But courts must conduct the class-certification inquiry before reaching a case's merits, so if the company's offer to Gomez will substantively undermine his claims down the line rather than rendering them moot at the outset, he will still have the chance to lead a class action. Having a class at his back would improve Gomez's negotiating leverage by raising the stakes thousands of times over for Campbell-Ewald.

Justice Stephen Breyer at one point seemed to verge on exasperation, characterizing the argument as hair-splitting.

"Fine," Justice Breyer told Mitchell. "Give him judgment on the merits. Who cares?"

"It's actually a very important distinction," Mitchell said.

"Why?" Justice Breyer responded.

"Because many reasons," Mitchell said.

"Well, give me one," Justice Breyer said, cutting Mitchell off a moment later to say, "I'm not interested in the 'question asked' (by the *certiorari* petition). I'm interested in the question I am asking."

Justice Breyer, a member of the court's politically liberal wing, also seemed to be looking for a way to address the "practical" question of why a company should have to go to the trouble of defending itself in court after voluntarily surrendering to the plaintiff.

> "This court has repeatedly said: When it's not necessary to decide, it's necessary not to decide," the plaintiff's attorney said.

Chief Justice John Roberts sounded the same theme, suggesting that allowing Gomez to lead a class action even with a complete settlement on the table would be a much bigger boon to plaintiffs' lawyers than to plaintiffs themselves.

"You won't take yes for an answer," the chief justice told Mitchell at one point.

'NECESSARY NOT TO DECIDE'

Campbell-Ewald's lawyer — former U.S. Solicitor General Gregory G. Garre, now of Latham & Watkins in Washington — also faced tough questions, but they came primarily from Justices Ruth Bader Ginsburg, Elena Kagan and Sonia Sotomayor, three of the court's more liberal members.

During one line of questioning, Justice Kagan sought to tease out whether Federal Rule of Civil Procedure 23 gives plaintiffs the procedural right to lead class actions or whether class actions are simply a device of convenience to save courts, businesses and consumers the costs associated with repetitive or duplicative litigation.

Justice Kagan repeatedly sought to reframe the issue. An individual settlement with a lead plaintiff in a class action can never actually offer "complete relief," she said several times, because one of the forms of relief the plaintiff wants is class certification.

Justice Ginsburg put a finer point on the idea.

Is there "a procedural right to litigate entitlement to class status?" she asked Garre.

"I don't think you can describe it as a procedural right," Garre said. "This court has said that Rule 23 is a procedural mechanism."

Garre, who argued first, seemed to anticipate the sorts of questions the justices would later direct at Mitchell, saying what matters most — technicalities aside — is that a plaintiff who rejects a complete settlement offer no longer has any case.

"[H]ere's our position," he said. "When the offer of complete relief is made and when a court has determined that it is, indeed, for complete relief, then the case has to come to an end. Now, whether you say it's moot at that precise moment or whether you say it starts the ball rolling down the hill ..., the point is that when the defendant has offered everything, the courts can't go ahead and expound on the law.

"[T]his court has repeatedly said: When it's not necessary to decide, it's necessary not to decide," Garre added. "And that's the fundamental principle at stake here." WJ

Attorneys:
Petitioner: Gregory G. Garre, Latham & Watkins, Washington

Respondent: Jonathan F. Mitchell, Stanford Law School, Palo Alto, Calif.

Home-sharing site, payment processor hit with data breach suit

By Melissa J. Sachs, Esq., Senior Legal Writer, Westlaw Journals

A site where homeowners can list short-term rental properties and its payment processor allowed hackers to access users' bank accounts and other personal information in breach of their security promises, according to a proposed class action filed in California federal court.

Bonnema v. HomeAway Inc. et al., No. 4:15-cv-05023, complaint filed (N.D. Cal., Oakland Div. Nov. 2, 2015).

HomeAway Inc. and payment processor YapStone Inc., doing business as VacationRentPayment, failed to reasonably safeguard users' sensitive information, leaving it vulnerable to hackers from about July 2014 through August 2015, site user Christopher Bonnema says in his suit filed in the U.S. District Court for the Northern District of California.

The proposed class action seeks more than $5 million in damages, relying on the Class Action Fairness Act, 28 U.S.C. § 1332(d), for jurisdiction.

The act gives federal courts jurisdiction over class actions that seek damages above $5 million, include more than 100 potential class members, and have diversity between a plaintiff and a defendant.

Bonnema is from San Luis Obsipo County, Calif., and HomeAway's headquarters are in Austin, Texas, the suit says.

Neither HomeAway nor YapStone responded to requests for comment on the allegations.

SECURE ELECTRONIC PAYMENTS?

According to the complaint, Bonnema listed rental property in the Dominican Republic on VRBO.com, another home-rental site that HomeAway owns.

About two years ago, he submitted an application to HomeAway Payments, which allows homeowners to accept electronic payments from renters, the suit says.

According to the suit, VRBO never mentions YapStone when describing HomeAway Payments, even though YapStone partners with HomeAway to process the payments.

Both companies allegedly promised to safeguard users' payment and personal information, including names, e-mail and physical addresses, birthdates, bank account information and Social Security numbers.

YapStone's website says the company stores users' payment information on secure servers and conducts rigorous annual audits to maintain the highest level of security, according to the complaint.

DATA BREACH

Despite the defendants' security promises, Bonnema received a notification letter in mid-September saying his financial and other personal information had been accessible to thieves through a YapStone website from about July 15, 2014, to Aug. 5, 2015, the complaint says.

Although the defendants knew about the security breach in August, they waited six weeks to notify affected website users and proposed class members, Bonnema says.

DAMAGES

The defendants' offer of 24 months of credit monitoring and identity theft insurance for affected customers is insufficient, the complaint says.

Credit monitoring services only notify enrolled individuals when new accounts are opened in their names, and they fail to prevent unauthorized charges made to existing accounts, the plaintiffs say.

Additionally, the notification letter recommends that potential identity theft victims incur out-of-pocket expenses by

placing a "security freeze" on credit reports or periodically reviewing these reports, which would cost money to maintain beyond one year, the plaintiffs say.

The suit alleges common law violations, such as negligence, breach of contract and unjust enrichment.

It also alleges violations of California's unfair-competition law, Cal. Bus. & Prof. Code § 17200, and the state's data breach law, Cal. Civ. Code § 1798.80. WJ

Attorneys:
Plaintiff: John H. Donboli and J.L. Sean Slattery, Del Mar Law Group, San Diego

Related Court Document:
Complaint: 2015 WL 6689586

See Document Section B (P. 35) for the complaint.

'Software as a service' not subject to Michigan use tax, state appeals court says

By Melissa J. Sachs, Esq., Senior Legal Writer, Westlaw Journals

A Michigan-based insurance company will get more than $870,000 in refunded taxes it paid under protest to the state for "software as a service" products, according to an appeals court decision.

Auto-Owners Insurance Co. v. Department of Treasury, No. 321505, 2015 WL 6473592 (Mich. Ct. App. Oct. 27, 2015).

Auto-Owners Insurance Co. disputed that the software-as-a-service, or SaaS, products were subject to Michigan's Use Tax Act, Mich. Comp. Laws § 205.91, and the state Court of Appeals agreed.

The law defines "use" in terms of ownership rights and, for various SaaS products at issue, the insurance company neither owned nor had ownership-type rights over the computer software or code, the appeals court's *per curiam* opinion said.

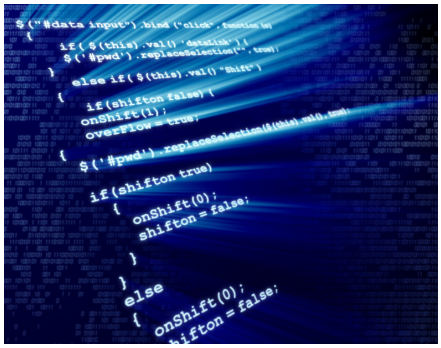
Auto-Owners sent electronic data or research requests to third-party service providers, which analyzed the information using computer code or software located on their servers and then returned the relevant results to the insurer, the opinion explained.

No physical transfer of property occurred, the opinion said.

For the other SaaS products, any software that Auto-Owners used or controlled was incidental to non-taxable services the insurance company purchased and should not have been subject to the use tax, the appeals court said.

This included services from companies such as LogMeIn, which allows employees to log into the company's network from their home computer; Cisco WebEx LLC, which provides Web conferencing services; and RT Lawrence, which processes payments, the opinion said.

While these third-party service providers may have required Auto-Owners to install apps on computers to access their services — meaning technically there was a transfer of property — the contracts with these companies were primarily for the services they offered, the appeals court explained.



It upheld the trial court's decision in favor of the insurance company and against the Department of Treasury.

June Haas, a tax partner at **Honigman Miller**, who represented Auto-Owners in the case, said the appeals court's decision gave more insight on how to handle SaaS products for tax purposes.

"This case is significant because Michigan is one of the first states to test the theory of whether 'accessing the functionality of software' located on a third party's server — such as through software as a service (SaaS) — is the same as purchasing software and subject to sales and use taxes by the state. The court held it is not and the transactions are not taxable," Haas said.

Michigan Treasury Department's communication director was not immediately available for comment.

USE VS. SALES TAX

According to the panel's opinion, Michigan's use tax complements the state's sales tax and targets transactions the sales tax does not cover.

Namely, it levies taxes for the privilege of using, storing or consuming tangible personal property, such as hardcopies of computer software, computer equipment, furniture or other goods, the opinion said, citing Mich. Comp. Laws § 205.93(1).

When a customer does not pay a sales tax for a good, generally they must pay a use tax for that item. Customers rarely remit use taxes on their own.

Usually, states require brick-and-mortar stores within their borders to collect and remit sales or use taxes from customers.

The switch to e-commerce and SaaS products has caused a problem for many states, which cannot enforce their tax regimes on out-of-state retailers and have lost significant revenue relying on customers to remit their use taxes.

AUTO-OWNERS' AUDIT

The Michigan Treasury Department audited Auto-Owners, which is headquartered in Lansing, for its use-tax liability from Dec. 1, 2006, to Dec. 31, 2010, the opinion says.

In 2012 it billed the insurer for past use-taxes and interest, the opinion said.

Auto-Owners entered into numerous contracts to which the Treasury Department determined the use tax applied, the opinion said.

These fell into six broad categories:

- Insurance-industry-specific contracts.
- Technology and communications contracts.
- Online research contracts.
- Payment remittance and processing support contracts.
- Equipment maintenance and software customer support contracts.
- Marketing and advertising contracts.

For example, Auto-Owners entered into a contract with West, a Thomson Reuters

business, which also owns Westlaw Journals, in order to conduct legal research through its online database service. The insurer never had access to West's computer code but merely submitted research requests through its online system, the opinion said.

Based on this usage, the panel found that Auto-Owners could not be assessed a use tax.

The opinion also noted two or three other contracts where a service provider had given Auto-Owners software to download onto its computers that the insurer controlled.

For example, Auto-Owners had to download and install software from LogMeIn, a company that provides services that allow employees to remotely access their work's network from home, the opinion said.

LogMeIn's software was incidental to the remote computing services that Auto-Owners bought, the opinion said.

For this type of contract, the transaction was principally for a provision of services, not for transferring property, and the incidental transfer of property did not qualify for the use tax, the appeals court said.

The Michigan Treasury Department has until Dec. 8 to file an application for leave to appeal to the state Supreme Court for discretionary review, Haas said in an email. WJ

Related Court Document:
Opinion: 2015 WL 6473592

DISCOVERY

Philips dodges discovery sanctions in trade secrets dispute

By Elizabeth T. Brown, Esq., Managing Editor, Westlaw Daily Briefing

A California federal judge has refused to find Philips in contempt for allegedly misusing confidential information disclosed during discovery in a federal suit in order to bring a trade secrets suit in California state court.

Koninklijke Philips NV et al. v. Elec-Tech International Co. et al., No. 14-cv-2737, 2015 WL 6449399 (N.D. Cal., San Jose Div. Oct. 26, 2015).

U.S. District Judge Beth Labson Freeman of the Northern District of California rejected Elec–Tech International Co.'s motion for civil contempt or sanctions because no enforceable protective order existed.

In a June 2014 federal complaint, Dutch electronics company Koninklijke Philips NV said an engineer with its San Jose, Calif.-based subsidiary Philips Lumileds Lighting Co., downloaded thousands of files containing trade secrets regarding Lumileds light-emitting diode technology and confidential business information just days before quitting his job with Lumileds.

After the engineer, Gangyi Chen, moved to China to work for Elec–Tech, he was immediately given a team of engineers and access to senior management, the complaint said.

Philips and Lumileds claimed that Elec-Tech developed its high-energy LED lighting products in an "unprecedented amount of time" given that the company had only entered the LED market in 2009.

The suit, brought against Elec-Tech, various of its subsidiaries, Chen and other individuals asserted nine state-law claims, including misappropriation of trade secrets under the California Uniform Trade Secrets Act, Cal. Cal. Civ. Code § 3426, and one count of violating the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C).

CASE DISMISSED

Judge Freeman ruled that the plaintiffs had failed to state a claim under the Computer Fraud and Abuse act against any of the defendants. *Koninklijke Philips NV v. Elec-Tech Int'l Co.*, No. 14-cv-2737, 2015 WL 1289984 (N.D. Cal. Mar. 20, 2015).

REUTERS/Francois Lenoir

U.S. District Judge Beth Labson Freeman refused to sanction Koninklijke Philips NV for disobeying a court discovery order because she found that no court order existed.

Without the CFAA claim, there was no basis for the court to exercise subject-matter jurisdiction, so Judge Freeman dismissed the entire suit with prejudice.

Four days later, Philips and Lumileds filed suit against the defendants in the Santa Clara County Superior Court.

According to the judge's most recent opinion, the state court suit alleges "nearly identical claims, but in greater factual detail."

In December Elec-Tech filed a motion for civil contempt or sanctions under Federal Rule of Civil Procedure 37(d) in the District Court.

NO ENFORCEABLE ORDER, NO CONTEMPT

During the original federal suit, the parties had orally agreed to be bound by the district's model protective order governing trade secrets and confidential information until they finalized a fully negotiated protective order. However, neither the parties nor Judge Freeman signed the model order, the opinion said.

The defendants claimed in their motion for contempt or sanctions that the plaintiffs had violated the model order by using documents subject to the order to draft the state-court complaint and possibly shared protected information with the Justice Department.

"Contempt requires the existence of a specific and definite court order," Judge Freeman wrote. But no such order existed in this case, she said.

Rather, the parties had merely reached an "interim agreement" to abide by the model order that they intended to serve as a "stop-gap measure" until they could agree on a final protective order, the judge said.

Because no court order existed, Judge Freeman refused Elec-Tech's request that she sanction Philips under Rule 37(b)(2) for disobeying a court discovery order.

Citing *Kokkonen v. Guardian Life Insurance Company of America*, 511 U.S. 375 (1994), the judge also refused to invoke the court's inherent power to sanction Philips for having violated the parties' private agreement after the federal case had concluded. WJ

Attorneys:
Plaintiffs: Benjamin D. Mooneyham, Brian D. Roche, Jennifer Depriest, Lawrence E. James Jr. and Steven A. Miller, Reed Smith LLP, Chicago; Kirin K. Gill and William R. Overend, Reed Smith LLP, San Francisco

Defendants: Claude M. Stern, James S. Tsuei and Michael D. Powell, Quinn Emanuel Urquhart & Sullivan, Redwood Shores, Calif.; Michael F. Peng, Quinn Emanuel Urquhart & Sullivan, Hong Kong; Minyao Wang, Quinn Emanuel Urquhart & Sullivan, New York

Related Court Document:
Order: 2015 WL 6449399

DECEPTIVE MARKETING

FTC settles with operators of alleged PC tech support scam

By Jason Schossler, Contributor, Westlaw Journals

The operators of a New York-based company have agreed to give up real estate and luxury cars to settle charges that they tricked consumers into paying hundreds of dollars for computer security and tech support services they did not need.

Federal Trade Commission v. Pairsys Inc. et al. No. 1:14-cv-01192, stipulated order issued (N.D.N.Y. Oct. 20, 2015).

Pairsys Inc. and its owners, Tiya Bhattachara and Uttam Saha, allegedly conned consumers into paying $149 to $249 for bogus services and computer software that was otherwise available for free, according to the complaint the Federal Trade Commission filed in the U.S. District Court for the Northern District of New York.

The company made nearly $2.5 million since early 2012 from the purported scheme, the commission said in a statement announcing the settlement.

The defendants agreed to a stipulated order that includes a monetary judgment of nearly $3.1 million, according to the FTC.

This amount is suspended pending the defendants' surrender of two real estate properties in Albany, N.Y., and leases on a 2013 Range Rover and a 2014 Maserati Quattroporte, the commission said.

The defendants also must forfeit unspecified funds held in multiple bank accounts, according to the FTC.

The order also bans the defendants from selling any tech support service to consumers, participating in telemarketing in general and making any advertising misrepresentations to consumers.

The complaint says the defendants lured consumers with deceptive online advertisements and made cold calls falsely claiming to be representatives of Microsoft or Facebook.

After gaining remote access to a consumer's computer to analyze purported security issues, the defendants would say the machines were infected with viruses or other malware, which in reality often did not exist, the suit said.

In furthering this alleged deception, the defendants led consumers to believe that certain innocuous files on their computers posed certain security risks and errors that needed to be addressed immediately, according to the suit.

Consumers were then pressured into paying for bogus warranty programs and antivirus software that was freely available, the FTC said.

The complaint accused the defendants of violating the Federal Trade Commission Act, 15 U.S.C. § 45, for unfair or deceptive acts, and the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. § 6101. WJ

SEC adopts long-awaited crowdfunding rules

By Cory Hester, Attorney Editor, Westlaw Daily Briefing

The Securities and Exchange Commission recently adopted final crowdfunding rules, the last of its major JOBS Act rulemaking mandates.

The final rules, known as "Regulation Crowdfunding," will allow smaller companies to raise capital through private offerings on SEC-approved online portals. Further, the rules will provide investors with various protections when executing securities-based crowdfunding transactions.

SEC chair Mary Jo White previously stated that the commission planned to implement final crowdfunding rules in a speech at the SEC Speaks program in February. She applauded the recent announcement, noting that "there is a great deal of enthusiasm in the marketplace for crowdfunding, and I believe these rules and proposed amendments provide smaller companies with innovative ways to raise capital and give investors the protections they need."

> Companies that qualify for crowdfunding offerings must make certain required disclosures under the new rules, including information about the methodology used to calculate securities' offering prices.

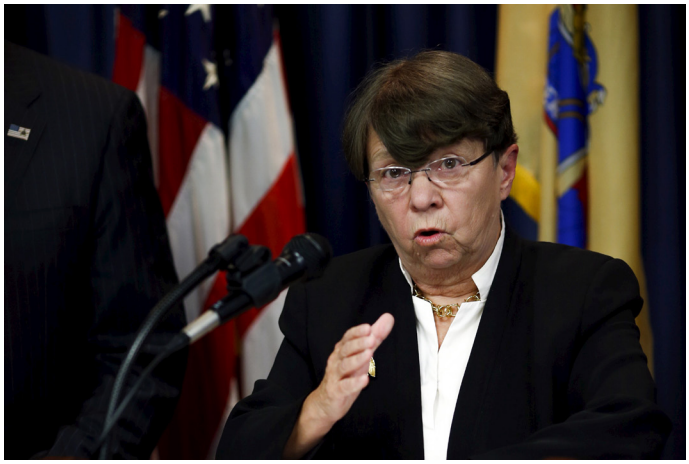
In addition to enabling individuals to purchase securities in crowdfunding offerings, the final rules will require that companies disclose certain information about their business and securities offering. The rules also create a regulatory framework for intermediaries that facilitate crowdfunding transactions.

The rules will place some limits on issuers' ability to raise money through crowdfunding transactions. For example, companies are not permitted to raise more than $1 million in proceeds through such offerings over a 12-month period.

For individual investors with an annual income or net worth of less than $100,000, the rules will permit the person to invest up to $5,000 over a 12-month period, or a maximum five percent of the lesser of their annual income or net worth.

The rules permit individuals who have both annual income and net worth equal to $100,000 or more to invest up to $100,000, or up to 10 percent of the lesser of their annual income or net worth.

Not all companies are eligible to use crowdfunding offerings, however. Issuers excluded from such offerings include, among others, non-U.S. companies, issuers that already file reports under the Securities Exchange Act of 1934 and certain investment companies.



SEC chief Mary Jo White REUTERS/Eduardo Munoz

Companies that qualify for crowdfunding offerings must make certain required disclosures under the new rules, including information about the methodology used to calculate the securities' offering price. Further, such issuers must disclose information about the company's financial condition, a description of the intended use of proceeds from the offering, information about the company's officers and directors, and information about certain related-party transactions.

Such companies are also required to file annual reports with the SEC.

The rules also introduce a regime to regulate online funding portals that issuers use to facilitate crowdfunding offerings, including mandating registration with the SEC on a new "Form Funding Portal." Such portals must become a member of a national securities association, currently FINRA.

Crowdfunding intermediaries are also required to, among other things, provide investors with educational materials, take certain measures to reduce the risk of fraud and provide information to investors about the intermediary's compensation arrangement.

Additionally, the rules prohibit intermediaries from engaging in certain transactions, such as allowing a crowdfunding offering through its platform of a company in which it holds a security interest.

The SEC stated that the new crowdfunding rules and forms will take effect 180 days after they are published in the Federal Register. The forms enabling funding portals to register with the Commission will be effective Jan. 29, 2016. WJ

CEO's fraudulent intent can be imputed to corporation, 9th Circuit rules

By Peter H. Hamner, Esq., Senior Legal Writer, Westlaw Journals

A CEO's intent to defraud investors by embezzling $120 million can be imputed to the corporation, making the company potentially liable for "textbook securities fraud," the 9th U.S. Circuit Court of Appeals has held.

In re ChinaCast Education Corp. Securities Litigation, No. 12–57232, 2015 WL 6405680 (9th Cir. Oct. 23, 2015).

Reversing a decision by U.S. District Judge John F. Walter of the Central District of California to dismiss the shareholder suit against ChinaCast Education Corp., the 9th Circuit held that the company cannot escape liability even though the CEO was responsible for the fraud.

According to the panel's opinion, ChinaCast is a for-profit education company that provides online and on-campus, college-level educational courses to students in China.

Problems began when the company disclosed in a March 2011 regulatory filing that its auditor had found internal control weaknesses regarding its financial oversight.

"The adverse-interest rule collapses in the face of an innocent third party who relies on the agent's apparent authority," the 9th Circuit said.

ChinaCast CEO and founder Ron Chan Tze Ngon allegedly stole about $120 million from the company between June 2011 and April 2012 by transferring corporate assets to outside accounts he controlled.

Meanwhile, Tze Ngon and CFO Antonio Sena had told investors during this period that the company maintained good financial health, and they reassured investors by downplaying the auditor's warning, the appeals panel's opinion says.

The company discovered Tze Ngon's fraud in March 2012 after he tried to interfere with its annual audit. It disclosed the fraud in regulatory filings, leaving it in "financial ruin," the opinion says.

Shareholders sued the company and its independent directors, alleging violations of Sections 10(b) and 20(a) of the Securities Exchange Act of 1934, 15 U.S.C. § 78j(b), and Rule 10b-5, 17 C.F.R. § 240.10b-5.

Judge Walter granted the company's motion to dismiss the suit. *In re ChinaCast Educ. Corp. Sec. Litig.*, No. 12–CV-4621, 2012 WL 6136746 (C.D. Cal. Dec. 7, 2012).

He ruled the CEO's action could not be imputed to the company, citing the "adverse interest" exception to securities law violations, which provides that the actions of employees that are adverse to their employer cannot be imputed to the corporation.

"In this case, there is no allegation that [Tze Ngon] or his accomplices acted out of anything other than their own self-interest or that their conduct in any way benefitted ChinaCast," Judge Walter said.

The 9th Circuit reversed.

"The adverse-interest rule collapses in the face of an innocent third party who relies on the agent's apparent authority," the appeals panel said.

Because Tze Ngon was CEO, the company "should have kept close tabs" on him. The auditor's warning also put ChinaCast on notice, the panel said.

Thus, shareholders relied on Tze Ngon's status as CEO and were innocent in the fraud, the 9th Circuit sasid.

"Significantly, imputation is proper because [Tze Ngon] acted with apparent authority on behalf of the corporation, which placed him in a position of trust and confidence and controlled the level of oversight of his handling of the business," the 9th Circuit said.

"Assuming a well-pled complaint, we recognize that, as a practical matter, having a clean-hands plaintiff eliminates the adverse-interest exception in fraud-on-the-market suits because a bona fide plaintiff will always be an innocent third party," 9th Circuit held. WJ

Related Court Document:
Opinion: 2015 WL 6405680

Impact of *ChinaCast* ruling

The import of the decision is that in future cases in which C-suite executives are allegedly accused of looting the company for their own self-interest, shareholders will have an easier job of pleading *scienter* under the federal securities laws to maintain a shareholder class action.

If the 9th Circuit had ruled the other way, shareholders would be limited to derivative shareholder litigation as their sole means to seek redress. Now, shareholders will be more likely to avail themselves of the class-action mechanism in addition to derivative litigation.

This will drive up litigation costs for companies likely already subject to investigations by the SEC and DOJ in addition to civil shareholder litigation. However, the decision will have very limited application only to the handful of cases filed every year that allege looting by C-suite executives.

–Sarah A. Good, partner, Pillsbury Winthrop Shaw Pittman LLP

Judge approves tentative $23 million deal in Zynga securities suit

A California federal magistrate judge has granted preliminary approval to a proposed settlement agreement in a securities class-action lawsuit against social-platform video game company Zynga Inc.

In re Zynga Inc. Securities Litigation, No. 12-cv-04007, 2015 WL 6471171 (N.D. Cal. Oct. 27, 2015).

The proposed pact would provide a $23 million fund for those who purchased Zynga shares following a Dec. 15, 2011, initial public offering and later suffered damages when the company revealed its finances were deteriorating, according to the order from U.S. Magistrate Judge Jacqueline Scott Corley of the Northern District of California.

The settlement is the product of 12 consolidated class-action suits for which David Fee is the lead plaintiff, the order said. The complaint alleged violations of Sections 10(a), 10(b) and 10b-5 of the Exchange Act against Zynga, CEO Mark Pincus, Chief Financial Officer David M. Wehner and Chief Operating Officer John Schappert.

> The proposed $23 million settlement represents an average distribution of 15 cents per share.

Fee claimed the individual defendants knew prior to the IPO that user numbers, spending and in-game purchases were declining. Within months of the IPO — and despite being time-barred from selling for a certain period — the individual defendants and others sold their shares for hundreds of millions of dollars in a secondary offering April 3, 2012, the investors said.

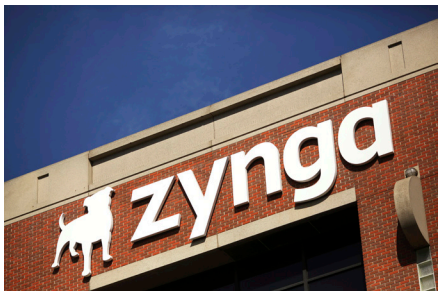
The judge's order said the company essentially shifted its revenue losses from the first quarter of 2012 to the second, allowing it to artificially inflate stock prices.

Zynga also released a series of false and misleading statements about financial transactions, changes to Facebook and its 2012 outlook, even as finances were crumbling, the order said. The company revealed its poor financial standing July 25, 2012, and stock prices tumbled 37 percent in a single day.

Following consolidation of the suits, Fee initially sought a class period running from Dec. 15, 2011, to July 25, 2012. This was shortened in a subsequent first amended complaint to just five months, running from Feb. 14, 2012, to July 25, 2012 — the period after the company's first 2012 guidance was released.

According to the order, Fee estimates he may receive 100,000 class member claim forms and that the average distribution would be 15 cents per share before fees and expenses are deducted. Lead counsel for Fee has already indicated they will seek $5.75 million in fees and up to $276,000 for expenses.

Fee also said he would seek $900,000 in claims administrator's expenses, according to the order. All told, this could account for 4 cents per share in distribution, the order said.



REUTERS/Robert Galbraith

Class members will receive distribution based on the number of shares held at various points in 2012 and can choose to opt out of the agreement within 70 days of receiving notice of the settlement. In the event there is leftover money in the fund, it will be given to a charity of Fee's choice, pending court approval.

The parties were able to reach an agreement in August, before the class was certified, and Judge Corley found the proposed class members and distribution plan were reasonable and fair.

Fee's counsel was ordered to file a motion for approval of attorney fees and costs within 40 days of notice being given to class members. Both parties are expected to return for a final fairness hearing Jan. 28, 2016.

Counsel for Fee was also ordered to file a motion seeking final approval of the settlement 35 days before that hearing. WJ

Related Court Document:
Order: 2015 WL 6471171

Facebook director compensation suit survives because CEO did not ratify plan

A shareholder suit over allegedly excessive pay for Facebook's outside directors can go forward because CEO Mark Zuckerberg, as the majority shareholder, did not formally approve the 2013 compensation plan, a Delaware Chancery Court judge has ruled in a first-impression opinion.

Espinoza v. Zuckerberg et al., No. 9745, 2015 WL 6501521 (Del. Ch. Oct. 28, 2015).

Chancellor Andre G. Bouchard said the Facebook directors' approval of pay increases for non-management board members, known as "outside" or "independent" directors, is not entitled to the deference of the business-judgment rule because Zuckerberg, as the 61 percent owner, did not officially ratify it.

It was the first time the Chancery Court had addressed the narrow issue of whether a single controlling shareholder is required to ratify a legally disputed action through either a stockholder meeting vote or by written consent like public shareholders.

> Since CEO Mark Zuckerberg's ratification was not valid, the defendants must show that their actions were entirely fair to the shareholders, and they have not done that, Chancellor Andre G. Bouchard said.

Chancellor Bouchard said the answer is yes. He refused to dismiss breach-of-duty and unjust-enrichment charges because the director defendants, including Zuckerberg, had not met their burden of proof that the pay plan was fair.

In response to a request for comment on the ruling, **Facebook** spokeswoman **Vanessa Chan** said, "We are reviewing the decision."

Under the corporate law of Delaware, where California-based Facebook Inc. is chartered, legally challenged board decisions are entitled to the benefit of the doubt unless the directors profit from them or stood on both sides of the deal in some way. In that case, the actions must be examined under the harsh light of the "entire fairness" doctrine, and the burden of proof shifts to the defendants to show that the shareholders were not shortchanged.

SAME RULES FOR ZUCKERBERG

If the majority of the shareholders ratify the action in a formal vote, it can still be sheltered under the business-judgment umbrella, but Zuckerberg only endorsed it during discovery for this derivative suit, the chief judge said.

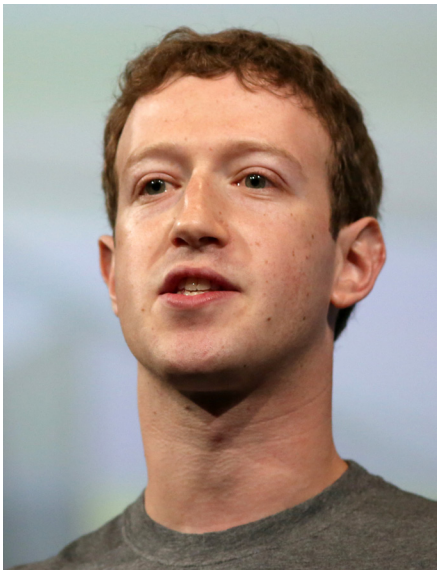
Chancellor Bouchard refused to dismiss claims by Facebook shareholder Ernesto Espinoza that the directors breached their duty to run the company efficiently and without conflicts of interest, finding that a question remains as to whether a majority of the directors were personally interested in the plan they approved.

The suit arose from Facebook's adoption of an equity incentive plan in 2012 to help retain and motivate employees, officers, directors and consultants with grants of company stock, according to the complaint. The pay was approved in 2013.

The EIP sets a total limit of 25 million shares of issuable stock to non-employee directors, with a yearly limit of 2.5 million shares to any one individual, the suit says.

At the time the suit was filed, those 2.5 million shares translated to roughly $145 million, which means the board is "essentially free to grant itself whatever amount of compensation it chooses," the complaint said, and Espinoza claims the board has done so.

According to the complaint, Facebook directors were paid an average $460,000 in 2013, about $140,000 more than the average per-director compensation offered at other companies in Facebook's "peer group."



REUTERS/Robert Galbraith

Chancellor Andre G. Bouchard said Facebook directors, including CEO Mark Zuckerberg, shown here, must face charges that they unreasonably approved "excessive" pay increases for non-management board members.

MORE PAY THAN PEERS?

The complaint points to a dozen companies in that group, according to Facebook's own public disclosures, including Amazon, Cisco, Netflix, Walt Disney and Yahoo. The peer average revenue for these companies is $22.9 billion, compared with Facebook's $7.8 billion, with net income of nearly $3 billion versus Facebook's $1.5 billion, according to the complaint.

Espinoza said most of this compensation came as stock awards approved in September 2013 but was unwarranted in light of Facebook's performance in the market.

He alleged that without judicial intervention, Facebook's board will continue to award itself undeserved and unreasonably high rates of compensation. He is seeking damages in favor of the company in the form of restitution and disgorgement, as well as an order directing Facebook to reform the 2012 EIP so that it contains "meaningful limits" on the amount of stock the board can pay itself.

Facebook and its directors filed a motion for summary judgment, arguing Zuckerberg's endorsement of the plan was enough to ratify the action and give it the deferential treatment of the business-judgment rule.

But Chancellor Bouchard found that since the CEO's ratification was not valid, the defendants must show that their actions were entirely fair to the shareholders. They have not done that, he said, and he refused to dismiss the breach-of-duty and unjust-enrichment charges.

NO WASTE OF ASSETS

However, Chancellor Bouchard said the legal test to properly charge waste of assets is very stringent and requires well-supported allegations that "the director defendants authorized an exchange that is so one-sided that no business person of ordinary, sound judgment could conclude that the corporation has received adequate compensation."

He dismissed that claim, noting that "plaintiff wisely refrains from alleging that the all-star cast on Facebook's board is so lacking in talent ... that Facebook receives nothing in return for compensating its members." WJ

Attorneys:
Plaintiff: Kathaleen St. J. McCormick and Nicholas J. Rohrer, Young, Conaway, Stargatt & Taylor, Wilmington, Del.; Brian J. Robbins, Felipe J. Arroyo and Jenny L. Dixon, Robbins Arroyo LLP, San Diego

Defendants: David E. Ross and S. Michael Sirkin, Ross Aronstam & Moritz, Wilmington

Related Court Document:
Opinion: 2015 WL 6501521

Olympics organizers

CONTINUED FROM PAGE 1

the plaintiffs say was "in reliance on Mr. Frayne's representations that he would use such domain names solely as a forum for discussion."

REACTION

Frayne's counsel in the 2008 suit, Chicago-based Daspin & Aument, has not been retained in the instant suit and did not comment on the litigation.

FairWinds Partners attorney **Steven Levy**, an arbitrator of domain disputes, said Frayne might say he intends to host sites for criticism or other fair uses, but "his pattern of registering the names and dates of Olympic cities along with his passive holding of these domains for a number of years could very well be used to show his lack of rights and his bad faith."

Bracewell & Giuliani attorney **Erin Hennessy** likewise views Frayne's pattern of registering Olympics-related domain names as appearing "to fall squarely within the 'bad faith' required for a successful claim" by the Olympic committees.

The defendant's "pattern of registering the names and dates of Olympic cities along with his passive holding of these domains for a number of years could very well be used to show his lack of rights and his bad faith," FairWinds Partners attorney Steven Levy said.

Bracewell & Giuliani attorney Erin Hennessy said the defendant's pattern of registering Olympics-related domain names appears "to fall squarely within the 'bad faith' required for a successful claim" by the Olympic committees.

Sideman & Bancroft attorney **Kelly McCarthy** called the case "interesting" because it might result in a significant extension of the Olympic committees' trademark rights.

The Olympic committees "could claim rights not only to those words and city-date combinations already designated for the Olympic Games, but also to any city-date combination which had the chance of ever becoming a site for the games," McCarthy said.

Levy, Hennessy and McCarthy are not involved in the litigation.

'MONETIZING ... THE OLYMPICS'

The IOC, based in Lausanne, Switzerland, and the USOC, based in Colorado Springs, have co-owned U.S. registrations for numerous trademarks combining city locations with past and future dates of the Olympic games, such as "London 2012" and "Tokyo 2020."

According to the complaint, Frayne and CityPure registered nearly 1,500 domains consisting of a city and an Olympic year combined with a generic top-level suffix such as ".com."

Frayne has registered domains with the names of cities that have previously hosted the games with future dates, such as Losangeles2040.com and Mexicocity2036.com, the complaint says.

The suit claims Frayne is following a trend, counting on cities to host games again because they are well-equipped and often rebid for the opportunity.

The complaint references an online video of Frayne admitting to making "money by monetizing the worldwide tremendous interest in the Olympics," and calling his domain purchases a "naming pattern."

CHICAGO 2016

In July 2008 the USOC, which owned a "Chicago 2016" trademark, filed a complaint with the World Intellectual Property Organization to obtain the domain Chicago2016.com from Frayne.

In September 2008 Frayne filed a suit in the U.S. District Court for the Northern District of Illinois that included allegations of reverse domain-name hijacking, that is bringing suit in bad faith to wrest a domain from its owner.

The District Court rejected Frayne's claim that the suit was a sham meant to silence any criticism of Chicago's bid for the Olympics. *Frayne v. Chicago 2016,* No. 08C5290, 2009 WL 3229625 (N.D. Ill. 2009). The case was settled in November 2009.

DISCUSSIONS?

The Tokyo2020 domain contains the phrase "A Balanced Discussion" and a reference to CityPure, but the page is otherwise blank.

Sideman & Bancroft attorney Kelly McCarthy called the case "interesting" because it might result in a significant extension of the Olympic committees' trademark rights.

While some of Frayne's domains consisting of city-date combinations resolve to Web pages titled "Future Discussions," they likewise contain no actual discussions, the complaint says.

The complaint says Frayne and CityPure have violated Section 220506(c) of the Olympic and Amateur Sports Act, 36 U.S.C. § 220506(c).

The defendants' online actions demonstrate a bad-faith intention to profit from another's trademarks in violation of Section 43(d) of the Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d), the complaint says.

Use of the plaintiffs' registered marks also violates Section 32 of the Lanham Act, 15 U.S.C. § 1114, the complaint says.

The plaintiffs seek an order directing Frayne and CityPure to transfer all of their city-date combination domains to the Olympic committees and an injunction preventing the defendants from registering any more of such domains.

The plaintiffs also seek statutory and treble damages, attorney fees and costs. WJ

(*Additional reporting by Melissa J. Sachs, Esq., Senior Legal Writer, Westlaw Journals*)

Attorney:
Plaintiffs: Rodney Caldwell, Pirkey Barber PLLC, Austin

Related Court Document:
Complaint: 2015 WL 6782842

See Document Section A (P. 23) for the complaint.

NEWS IN BRIEF

N.Y. FEDERAL COURT FINDS NO INFRINGEMENT FOR 2 E-BOOK DOWNLOADS

Barnesandnoble.com has defeated a copyright infringement suit filed in New York federal court over two downloads of an e-book sample pulled from its online store. After writer Louis K. Smith's agreement with his distributor ended, one Barnes & Noble customer downloaded samples of his e-book to two digital devices, the opinion said. Barnes & Noble had pulled Smith's e-book from its online store, but it never deleted the previously requested sample from the customer's digital locker, a cloud storage method, the opinion said. Smith sued the online retailer for direct and contributory copyright infringement, and his widow, Cheryl, later took over as plaintiff in the suit. Barnes & Noble did not reproduce or distribute the e-book volitionally, plus its e-book reader and digital locker had legitimate, noninfringing uses, the judge said, finding the retailer could not be liable for direct or contributory infringement. Smith filed a notice of appeal the same day.

Smith v. Barnesandnoble.com LLC, No. 12-cv-4374, 2015 WL 6681145 (S.D.N.Y. Nov. 2, 2015).

Related Court Document:
Opinion: 2015 WL 6681145

MOVIE BIZ FREELANCER SUES HOLLYWOOD REPORTER OVER SONY DATA BREACH STORY

A freelance production accountant who worked on "The Amazing Spider-Man" has sued Prometheus Global Media Inc., parent company of The Hollywood Reporter, in Illinois federal court, alleging the news outlet wrongfully accused her of participating in Sony's recent data breach. Nicole Basile, who lives in Manhattan, Ill., says journalists Gregg Kilday and Tatiana Siegel, also named defendants, published the defamatory article in The Hollywood Reporter's magazine and on its website. The article wrongfully portrays her as a disgruntled employee with administrative access to Sony's servers, the suit says. Basile never worked directly for Sony, and the writers never reasonably tried contacting her before publishing the defamatory article, the suit says. Basile says the article has prevented her from getting work and caused her severe emotional stress. The complaint includes counts for libel per se and false light. Basile seeks over $75,000 in damages.

Basile v. Prometheus Global Media LLC et al., No. 15-cv-10138, complaint filed (N.D. Ill., E. Div. Nov. 6, 2015).

Related Court Document:
Complaint: 2015 WL 6867810

RESTRICTED PAYPAL USERS' $3.2 MILLION SETTLEMENT OK'D

A $3.2 million settlement of a class action accusing PayPal of unilaterally placing holds on users' accounts has received a California federal judge's preliminary approval. PayPal allegedly restricted a class of accountholder plaintiffs headed by Moises Zepeda from accessing their money after it found they breached their user agreements, either by selling counterfeit goods or providing false or inaccurate information, the judge said. PayPal never specified the wrongdoing or provided restricted accountholders with an opportunity to cure the freeze, the judge found. The accountholders sued for various common law and statutory claims, including breach of contract, and the parties negotiated a settlement for more than two years. The judge rejected the initial agreement but found the current settlement fair and adequate. It sets aside $1.84 million of the $3.2 million fund for class claims. A final hearing will be held in about nine months.

Zepeda et al. v. PayPal Inc. et al., Nos. C 10-2500 and C 10-1668, 2015 WL 6746913 (N.D. Cal. Nov. 5, 2015).

Related Court Document:
Order: 2015 WL 6746913

CASE AND DOCUMENT INDEX