epiq teamwork

Understand and Prepare for Health-Care Data Breach Class Actions

People. Partnership. Performance.

Understand and Prepare for Health-Care Data Breach Class Actions

The Identity Theft Resource Center, a nonprofit assisting business and individual victims of identity theft, calculated that 932 U.S.-based data breaches were reported between Jan. 1 and through Sept. 2018 in banking, government, education, health care, and business. Data breaches have been increasing steadily since 2005, though the method of breach has changed significantly as hacking has become more sophisticated.

A decade ago, targeted intrusions into data networks represented 14 percent of breaches. By mid-2017, hacking caused 63 percent of data breaches, with phishing accounting for approximately half of reported incidents. ITRC has also noted a significant rise in "CEO spear phishing"—the use of e-mails that mimic e-mails from business leaders—and reporting of ransomware attacks that began in 2016.

> **"A decade ago, targeted intrusions into data networks represented 14 percent of breaches. By mid-2017, hacking caused 63 percent of data breaches."**

Because employees can unwittingly click on links in phishing or ransomware e-mails, causing companies to lose control over data, business leaders must mitigate risk by developing strategies and plans for data breach prevention, protection, and resolution. In addition, they should prepare for data breach scenarios and obtain cyber insurance protection.

Health-Care Industry Breaches Rank Second

Of the more than 900 data breaches so far in 2018, 259 were in medicine or health care. That number represents 12 percent of all records compromised this year. Health-care breaches are the second-highest type, with business breaches (retail, tourism/service industry, excluding banking/credit/financial breaches) representing the greatest number of occurrences.

The medical and health-care industry provides the most accurate tracking of the number of records compromised, likely attributable to the Health Information Technology for Economic and Clinical Health Act, which requires reporting of breaches affecting 500 or more individuals to the Department of Health and Human Services. The law mandates public notification of security breaches when "unsecured protected health information" is disclosed or used for an unauthorized purpose.

In general, the HITECH Act requires that patients be notified of any breach of their data security, whether external or internal. If HHS is notified of a breach, the name of the institution where the breach occurred will be posted on the HHS website, and under certain conditions, local media will also need to be notified.

Class Action Data Breach Lawsuits

A 2017 report issued by Bryan Cave found ninety-five percent of lawsuits for all types of data breach alleged negligence, and 88 percent of lawsuits alleged a breach of sensitive data, which includes

information such as Social Security numbers or medical treatment information. Seventy-six class-action data breach lawsuits were filed in 2016, and some 34 percent of these involved the medical industry.

Class Action Certification Rules

Class actions are an exception to the general rule that litigation is conducted by and on behalf of the individual named parties only. To depart from that general proposition requires that the person or persons designated as class representative(s) must be a part of the class, possess the same interest, and suffer the same injury as the class members.

Federal Rule of Civil Procedure 23(a) ensures that the named plaintiffs are appropriate representatives of the class whose claims they wish to litigate. The rule's four requirements—numerosity, commonality, typicality, and adequate representation—ensure that the class claims are encompassed by the named plaintiffs' claims.

If Rule 23(a) is satisfied, plaintiffs must then meet one of the three subsections of Rule 23(b) to proceed. Under 23(b)(1), a class action can be maintained if separate actions would create a risk of establishing inconsistent standards of conduct for the party opposing the class, or if separate lawsuits could determine the interests of non-parties.

Under Rule 23(b)(2), a class action may be maintained if the class seeks injunctive or declaratory relief. These class actions can proceed if damages are incidental to the relief and computed by objective standards. Rule 23(b) class actions do not require a notice period to opt out.

Lastly, Rule 23(b)(3) permits certification when the primary relief sought is damages. Rule 23(b)(3) requires that common questions of law and fact predominate over any individual questions, and that a class action be superior to other methods for fair and efficient resolution of the conflict. The Supreme Court has commented that the purpose of a 23(b)(3) class is to vindicate the rights of those claimants who, individually, would be unable to bring their claims against opponents in court.

Rule 23(b)(3) class actions must meet two additional requirements not present in other class actions: predominance and superiority. The court must find that common class questions predominate over individual issues and that the class action is the superior device for adjudicating the claims. Rule 23(b)(3)'s predominance criterion is more demanding than the requirements of 23(a).

Unlike (b)(1)-(2) classes, (b)(3) classes require notice and a chance for individuals to opt out of the action.

Risk of Future Harm and Constitutional Requirements

When a data breach class action lawsuit is filed, the first defense is often to challenge the plaintiff's standing—the ability of the plaintiff to vindicate rights in federal court. The minimum requirements for standing under Article III of the Constitution consist of three elements: a plaintiff must have suffered an injury-in-fact, the injury must be causally connected to the challenged action of the defendant, and the injury must be redressable by a favorable decision.

To meet standing requirements, plaintiffs must allege injury that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." The Supreme Court examined the injury requirement in 2013 in *Clapper v. Amnesty International USA* to determine whether the risk of future injury satisfied Article III, and stated that "allegations of possible future injury are not sufficient."

However, a footnote stated that the injury requirement does not always require that plaintiffs demonstrate that their injury will occur. The footnote suggested that in some instances, substantial risk that the harm will occur may be enough. Since the *Clapper* decision, the Sixth, Seventh, and Ninth Circuits have held that an objective likelihood of increased risk of future harm can suffice as an injury in fact to support standing while the Third and Fourth Circuits disagreed.

With respect to standing in health-care data breach class actions, practitioners and executives should note that on Feb. 16, 2018, the U.S. Supreme Court denied a certiorari petition that would have addressed the circuit split regarding future harm. CareFirst had appealed the D.C. Circuit's decision in *Attias v. CareFirst, Inc.*, in which the court held that the threat of harm from a data breach is enough to satisfy the injury-in-fact standing requirement.

Preparing for Data Breach Litigation

Until the Supreme Court resolves the circuit split regarding future harm, executives and practitioners can take steps to prepare for and mitigate risks related to data breaches and litigation.

Defending against class action lawsuits involves adopting appropriate cybersecurity measures, including training and education for staff, in addition to systems security. Preparation also includes assuming a data breach will occur and being prepared to move quickly to comply with any breach notice requirements imposed by various federal and state laws and regulations.

Even before a lawsuit is initiated, companies should search for qualified counsel to defend against anticipated lawsuits. Additionally, qualified vendors for class certification activities and for document retention, management, and discovery should also be retained, along with experts on the merits of potential damages claims.

Data breach lawsuits are becoming a given.

worldwide resourcefulness

Epiq, a global leader in the legal services industry, takes on large-scale, increasingly complex tasks for corporate counsel, law firms, and business professionals with efficiency, clarity, and confidence. Clients rely on Epiq to streamline the administration of business operations, class action and mass tort, court reporting, eDiscovery, regulatory, compliance, restructuring, and bankruptcy matters. Epiq subject-matter experts and technologies create efficiency through expertise and deliver confidence to high-performing clients around the world. Learn more at www.epiqglobal.com.

80+ offices 14 data centers 5,500+ people

epiq

People. Partnership. Performance. epiqglobal.com

Class Action & Mass Tort | Court Reporting | eDiscovery | Business Process | Regulatory & Compliance | Restructuring & Bankruptcy