Privacy & Data Security Law News

Online Shopping, Pandemic Elevate Legal Risk for E-Retailers

By Jake Holland

Nov. 25, 2020, 12:05 PM

- Credit card skimming, spoofing hits aim to steal consumer data
- Retailers may face lawsuits, enforcement following cyberattacks

As consumers opt for online purchases in lieu of crowded malls and long in-store lines during the coronavirus-impacted Thanksgiving holiday, the threat of data breaches and digital malfeasance looms large, cybersecurity experts and attorneys say.

“It’s an opportune time for bad actors, conducting an attack while the victim is distracted with eating turkey and watching football,” said David Springer, an attorney at Bracewell LLP in Austin, Texas.

Aside from causing headaches for consumers, cyberattacks tied to e-commerce sites or mobile applications could open businesses up to legal liability in the form of lawsuits or regulatory enforcement actions.

Companies should take a hard look at their security systems and gird for heightened cyber-risk during the holiday season, experts say. They could find themselves in a weakened position in the event of a breach lawsuit if they don’t, said Curtis Dukes, executive vice president and general manager of security best practices at the Center for Internet Security.

“Organizations are going to have to demonstrate that they’ve done the right things and established basic cyber hygiene programs,” Dukes said. “A court of law is more likely to find them liable if they don’t meet that standard duty of care.”

Heightened Risk

Bad actors have already sought to exploit the pandemic and infiltrate companies’ and individuals’ security systems, said Linn Freedman, a privacy and cybersecurity partner at Robinson & Cole LLP in Providence, R.I. That threat is exacerbated, she said, by the volume of data generated during the online shopping season, especially given stay-at-home advisories and consumer reluctance to shop in-person.

Hackers often spoof well-known companies' websites in a bid to get unsuspecting shoppers to enter their personal and financial data, Freedman said. They can also conduct ransomware attacks or send phishing emails to employees who inadvertently enable hackers.

Credit card skimming resulting in the theft of financial data is also a big risk with online shopping, Freedman said. Retailers that operate e-commerce sites should ensure compliance with Payment Card Industry standards to help mitigate the risk of such attacks.

"We're just seeing so many class action cases that it's going to be very challenging to defend your company if it's not PCI-compliant or hasn't done a security risk assessment of its online platforms," Freedman said.

And if a company experiences a data breach, it could find itself subject to fines under the California Consumer Privacy Act or the EU's General Data Protection Regulation, Dukes said. A breach can also serve as a blow to that retailer's brand.

"People are going to think twice about whether they want to deal with that website and conduct e-commerce with them," Dukes said.

Regulators such as the Federal Trade Commission and the Securities and Exchange Commission are on the lookout for companies who aren't forthright with how they handle their data, Springer said. State enforcement agencies can target companies for deceptive trade practices, such as saying they use data in one way but actually use it in another, he said.

Although enforcement actions can happen at any time, the risk is elevated in the event of a cyberattack or breach.

"Once something happens, an actual breach or a suspected incident, you're being looked at under the microscope," Springer said.

Best Practices

Retailers today aggregate massive volumes of data, keeping information that goes beyond payment data and that can include browsing and purchase history, Springer said.

Companies should take a hard look at what they're collecting and reduce potential liability by curtailing the volume of information they're acquiring, he said.

"Don't retain data you don't need," Springer said. "Someone can't steal what you don't have."

Security for mobile shopping, including through applications, is often not as prioritized as it should be, said Justin Lie, CEO of Singapore-based cyber-risk intelligence company SHIELD.

Businesses should invest more in mobile security and close gaps in their systems to guard against risks during the holiday shopping season, Lie said. This is especially important as shopping on smartphones becomes increasingly popular in the U.S., he said.

Consumers may have a hard time holding companies liable for spoofing attacks since the impersonated website into which the consumer enters data is the result of a bad actor's work and not necessarily due to a company's security flaws, Freedman said. But businesses should remain vigilant and shore up systems to reduce the risk of an attack or breach, both of which can put companies on the line for millions.

"Prevention on the front end is the best risk mitigation strategy," to minimize liability and legal headaches down the line, Freedman said.

To contact the reporter on this story: Jake Holland in Washington at jholland@bloombergindustry.com

To contact the editor responsible for this story: Melissa Robinson at mrobinson@bloomberglaw.com; Kibkabe Araya at karaya@bloomberglaw.com

Law Firms

Robinson & Cole
Bracewell LLP

Topics

class actions
phishing
malware
financial institution data security
enterprise risk management
hacking
financial data privacy
coronavirus
consumer privacy
data breaches
state privacy legislation
online sales
extortion
credit cards
mobile applications
General Data Protection Regulation
email

More from Bloomberg Law

Latest Stories in Privacy & Data Security Law News