SECURITY SELLS

Consumers entrust DR marketers and retailers with sensitive personal details, and they count on brands to keep that information safe.

By Ian P. Murphy

Cybercrime became big business last year. With large-scale hacks that affected Dropbox, LinkedIn, Yahoo, Oracle, and even the IRS, the problem has reached crisis-level proportions. Add the fact that Russian hackers may have influenced the outcome of the U.S. presidential election by stealing and leaking confidential e-mails, and the problem seems even more sinister.

While no direct response marketer has yet been implicated in a large-scale hack like the one that hit Target in 2013, a report from Dutch cybersecurity researcher Willem De Groot says that more than 6,000 online shopping sites were breached using malicious software to tap customer payment information last year alone. And brick-and-mortar and e-commerce storefronts alike are being targeted by credit card "skimming" operations.

For direct response marketers selling goods and services in an omnichannel marketplace, the question is not *if* a cyberattack will compromise their data, but *when* and how much. With big data linking payments, advertising, inventory management, and other information, a breach can cause big headaches if a marketer isn't prepared. Not only can a breach cost millions of dollars in lawsuits and other direct costs, it can also affect customer relationships if the payment and other information they shared is exposed.

"Data breaches that involve the compromise of consumer information pose multi-dimensional challenges for the victimized company," says Craig A. Newman, a partner with New York City-based Patterson Belknap Webb & Tyler LLP and chair of the firm's privacy and data security practice. "It's a balancing act of sorts—remediating the breach, minimizing the impact, and taking steps to reassure your customer base."

The High Cost of a Cyberattack

The average cost of a data breach was $7 million among companies surveyed by IBM and the Ponemon Institute, a cybersecurity research firm, for the 2016 *Cost of Data Breach* study. Among retail enterprises, the average cost per lost or stolen consumer record was $200, up $28 from the previous year.

While cybercriminals are responsible for half of all reported breaches, lawsuits and regulatory actions often blame the executives of public companies with the failure to exercise the appropriate fiduciary responsibility and oversight of data security.

In *FTC v. Wyndham Worldwide Corp.*, the commission charged that the hotel chain's security practices were unfair and deceptive, citing three security breaches experienced in 2008–2009 that exposed customers' personal and financial data and resulted in $10 million in fraudulent charges. While the company challenged the allegations, an appeals court ruled that Wyndham could be held accountable for weak security protocols—and effectively gave the FTC ongoing enforcement responsibilities.

"The law has always imposed responsibility on companies for the care of their customers," UC-Berkeley law professor Chris Hoofnagle told *Wired* magazine following the decision in 2015. "Data is just something new that companies have to protect if they want to bear the benefits of collecting it."

Consumer class action suits are increasing, too. "It's also an evolving area of law with consumer class actions filed in the aftermath of a breach," Newman says. "The courts are focused on the extent to which a consumer suffers a tangible injury as a result of the breach. Without that, many courts are reluctant to let consumers pursue claims."

Blamed for a Breach

Up to two-thirds of the costs involved in addressing a breach are indirect, however, and related to increased customer churn. Consumers know that there are security risks online, but they place responsibility for protecting their own personal data with the companies to which they give it, according to the *2016 Data Breaches and Consumer Loyalty Report* from Gemalto, an international data security firm.

The majority of the 9,000 consumers surveyed say they would stop using a retailer (60 percent) or social media site (56 percent) if it suffered a breach, according to the report, while 66 percent say they would be unlikely to do business with an organization that experienced a breach in which their financial

Tech Set to Enhance Payment Security

By Curtis Kleinman

Watching *The Jetsons* on TV in the late 1960s, I never thought that 50 years later, we'd still be flying cross-country at the same speeds and in the same type of airplanes. Most personal identification technology has been available for more than 30 years, too. But new technologies are about to become widespread in payment processing.

In 1982, when I was a college intern at the data center for Con Edison, the New York City utility company, they scanned my fingers for identification. Today at the gym, I look into a device, it scans my iris, and the door opens. Iris, facial, and fingerprint recognition technologies are available today for online and retail card-present purchases alike. Many people already log on to their computers and cell phones this way.

In the next decade, credit cards will likely be replaced by biometric personal identification technologies—iris, facial, and fingerprint scans. And refinements to these technologies will extend beyond transacting; you'll be able to use a unique physical characteristic as your house key, car key, passport, driver's license, and more. Consumers won't need to carry a thing, but they will have to be open to technology that "reads" information from their bodies.

Will this feel like an invasion of privacy? Perhaps. But such technologies may assist in preventing fraud, and consumers may be willing to share biometric information more readily if they can be assured of greater security. The problem is that those who commit acts of fraud are becoming as technologically advanced as the institutions guiding and guarding transactions.

Consumers may be willing to share biometric information more readily if they can be assured of greater security.

Chip Technology and Fraud

Chip-and-PIN technology will soon make it easy for even non-credit card holders to make purchases. Compared to the magnetic stripe, chip technology is more secure, and makes it tougher to tap a cardholder's sensitive information. But chip technology is just one small step in the fight against fraud; it falls short of the best potential fraud detection technology available today.

The problem is to match the card with the cardholder's personal information; once a card is stolen, protecting a cardholder's information gets more difficult. Hackers have clever ways to lift the cardholder's personal information from a card for their use.

This issue is so important that is has caused me to alter my way of doing business. When merchants apply for payment processing, I discuss their refund policies: Are customers refunded their money before the company gets the product back, for instance? A complete chargeback management strategy, including alerts and fraud-prevention tools, is crucial to merchant success.

Just Over the Horizon

In the near future, one or more of the recent advancements in payment technology will become commonplace. Instead of swiping, consumers will tap their phones to a card reader—as they already do at Starbucks and other retailers. They'll get an instant email or text message receipt, helping detect fraud quickly if they didn't initiate the transaction. Consumers will be able to use one card for business purchases, then push a button and switch to a personal credit or debit card.

Soon companies will introduce a number of innovations that make transacting easier and (hopefully) more secure. There will be a wireless chip that attaches to one's cell phone. More than one consumer account will be managed with a single piece of plastic. The credit card of the future will have multiple computer chips, buttons, and LED light displays, or simply be stored inside a smartphone or dedicated display.

As with *The Jetsons,* we may be surprised at how long some of these innovations take to become widespread. But with the pace of change accelerating, and digital and card-not-present transactions becoming the rule rather than the exception, chances are that we won't recognize the dominant payment technologies that are just a few years off—but they'll recognize us.

Curtis Kleinman is director of sales at Visopay, a payment processor based in Miami. He has 30 years of experience in banking and has authored dozens of educational articles and the e-book Show Me the Money. *He can be reached via email at curtis@visopay.com or by phone at (310) 573-9019.*

and sensitive information was stolen.

But while 58 percent of consumers expect to be the victim of a breach at some point, they place 70 percent of the responsibility for protecting that data with the seller. "Consumers have clearly made the decision that they are prepared to take risks when it comes to their security, but should anything go wrong, they put the blame on the business," says Jason Hart, senior vice president and CTO for data protection at Gemalto.

In the United States, 78 percent of consumers say they would switch to another business if a breach affected them directly, according to a separate survey from market intelligence firm IDC. "Consumers can exact punishment for data breaches or mishandled data by changing buyer behavior or shifting loyalty," says Sean Pike, IDC analyst.

Attack and Response

In the event of a breach, marketers should have a step-by-step incident response plan ready. In addition to conducting a range of internal IT analyses, the affected company will need to have a communications strategy in place that alerts regulators at FTC, SEC, and other regulatory bodies, while reassuring customers that you continue to have their best interests in mind.

Companies suspecting that there has been a data breach—noticing unusual online or mobile activity, a spike in customer complaints of identity theft, or a lost laptop or thumb drive that contains sensitive information—should act fast to mitigate losses, according to the FTC's *Data Breach Response: A Guide for Business*.

Take affected equipment offline, monitor IT access points, and change password and login information, FTC says. Then, notify law enforcement, partners that may have been affected (including banks, call centers, and fulfillment providers), and customers whose data may have been compromised. The faster you act, the less severe the damage

will be to the company, its marketing ecosystem, and its customer base.

If your company is unlucky enough to have a large-scale breach of customer financial information, a fast, conscientious, and concerned response will go a long way toward keeping customers. Consider offering preferred customer status, a goodwill offer, and a year's worth of free credit monitoring. Consult *FTC.gov* for additional tips.

The Challenge Ahead

Unfortunately, preventing a data breach isn't getting any easier. "Preparing for a data breach has become much more complex over the last few years," said Michael Bruemmer, vice president of Experian Data Breach Resolution, in a recent report. "Organizations must keep an eye on the many new and constantly evolving threats and address these threats in their incident response plans."

Malicious attackers may resell stolen user names and passwords, Experian says; since consumers often reuse passwords, this can lead to individuals being targeted with hacks on other accounts outside the original leak, or so-called "aftershock" breaches. Uneven adoption of chip-and-PIN (EMV) cards means that cyberattacks affecting payments will likely escalate in 2017, but spread to smaller companies that are slow to update software technology or share distribution and infrastructure networks.

And—following the election—Experian predicts that state-sponsored attacks may escalate from fraud and espionage to all-out cyberwarfare in 2017. "These conflicts will tend to leave consumers and businesses as collateral damage," the report says. "[They] will undoubtedly place critical infrastructure in the crosshairs, potentially leading to widespread outages or exposed personal information that could impact millions of innocent consumers."

Businesses should prepare for disruptions by purchasing data insurance and reviewing and strengthening both internal and consumer-facing security measures. They should also publicize and promote these efforts to consumers to show that even in the event of a breach, every effort was made to protect data.

"With the impending threats of consumers taking legal action against companies, an education process is clearly needed to show consumers the steps they are taking to protect their data," Hart says. "Implementing and educating about advanced protocols like two-factor authentication and encryption solutions should show consumers that the protection of their personal data is being taken very seriously."