worldpay
from FIS

PROTECTING CUSTOMER TRUST

PROTECTING YOUR MOST VALUED ASSET

As soon as a customer engages with a retailer or any type of business, the company instantly takes on a vital responsibility: protecting the customer's personal data. Today, cyberattacks and data breaches not only have financial consequences, they run the risk of losing the most important asset in any organization—customer trust.

This report begins by highlighting how data is being used and why that elevates the protection of data to an existential importance. We'll touch on risks and rewards of managing data assets in such a high-pressure environment. Finally, we'll look at the technologies retailers are using to protect their customers' data and future trends on the horizon including the use of Artificial Intelligence.

WHY RETAILERS COLLECT CUSTOMER DATA...

In the retail world we often talk about the importance of providing outstanding and personalized customer experiences. Privacy and security is also top-of-mind among those responsible for the success of retail organizations. But it's vital to link the two discussions to understand why protecting customer data is so important today.

Retailers collect and manage more types of customer data than ever because it represents the core materials used to capture payment and craft the personalized customer experiences essential to successful retailing in a mobile-first world. Retailers also collect customer data because it's essential to their mission of creating loyalty for their brand. Take for example, data from fitness apps that may offer diet and workout information to enhance the overall fitness experience. This type of service allows retailers to retain and grow their business by identifying what interests their clientele.

Additionally, that data can help retailers put a better plan together to provide incentives or coupons designed to provide rich and seamless customer experiences specifically tailored for that consumer. It's this personal data that most of us can intuitively recognize as requiring greater care.

What's exciting today is the growing ability to make meaningful connections between seemingly unconnected data points. Retailers are developing the skills to craft customer experiences that go beyond their needs to surprise and delight customers like never before.

... WHY TREATING THAT DATA RESPONSIBLY MATTERS

Building better consumer experiences is central to the core business strategy of every retailer.
A brand's reputation and credibility is beyond critical in a competitive and expanding retail market. Retailers strive to provide a positive, rich experience but if they don't protect customer data, it brings them up for reputational risk.

Trust with your customers is fundamental to success. When organizations have data breaches or incidents, even the most loyal customers will find their way to your competition. Consider just a few data points on consumer sentiment related to data breaches at retailers:

- A 2017 PwC report found that 85% of consumers won't shop at a business if they have concerns about their security practices.
- A 2018 "Brand Trust Survey" found that 48% of U.S. internet users try to buy exclusively from companies they believe will protect their personal data.
- A 2019 Verizon study found that 69% of survey respondents would avoid a company that had suffered a data breach. 29% of those surveyed would never visit that business again.

THE IMPORTANCE OF COMPLIANT THIRD-PARTY SERVICE PROVIDERS

Retail organizations generally aren't the only ones collecting data and creating rich database tables. They often go to a third-party service provider for demographic, behavioral and other data points. That's where we're starting to see a lot of risk: attackers are increasingly taking advantage of trust between data or analytics providers and their retail customers.

Threat groups exploit this trust and attack these third parties. They can target a service provider that has access to hundreds, if not thousands, of retail organizations as customers. An attacker's ROI is far greater pursuing third parties collecting this type of data than individual organizations.

Recently, eCommerce retailers have come under sustained attacks from a third-party campaign that targets customer service chatbot clients. Hackers inject malicious code to the chatbot client and the client is then embedded onto the checkout page. Because the merchant trusts the chatbot client, the client is infected, and the attacker walks away with cardholder data and personal information.

Third party data services are increasingly essential components in providing more compelling customer experiences. Whether they're a payment service provider, ISP, POS software, loyalty, marketing or any other third party, they need to be vetted continuously. Take the time to insure they're protecting your data and that they're meeting top quality data collection and storage practices and adhering to any industry standards that are in place such as PCI DSS compliance for storage of payment related data.

HOW CAN RETAILERS PROTECT THEIR CUSTOMERS—AND THEMSELVES

It's not easy to protect customers if you're a retailer today in the U.S., especially if you process or store cardholder personal and payment-related data. The U.S. leads the world in attacks and there are no signs of a slowdown on the horizon.

- The 2018 Thales Data Threat Report Retail Edition found that half of all U.S. retailers had been breached in the past year, with 3-in-4 having suffered a breach historically.

- Ponemon Institute's 2018 Cost of a Data Breach Study estimates that the average cost of a data breach globally exceeded $3.86 million, with the costs to U.S. companies by far the highest at an average of $7.91 million.

- Symantec estimates that 4800 websites each month are compromised by form jacking attacks in 2018.

The good news is there has been a positive uptick in merchants that are getting smart about protecting consumers by deploying technology such as point-to-point encryption and tokenization. Point-to-point encryption is designed to protect data at the point of capture and in motion. Encryption helps protect cardholder and other personally identifying transaction data as it makes its way through the financial system. Tokenization goes a step further by removing cardholder data from the retail environment and replaces the personally sensitive cardholder data with tokens.

Attackers are ultimately going after payment card data through different points of vulnerability. With so many ways to accept payments today: in-store, online, through mobile apps retailers need to stay protected in every channel and on every device. Encryption and tokenization are solutions proven to reduce risk while preserving essential business functions and serving today's consumer.

Tokenization solutions make it possible for the retailers to operate their business without all the risk. Using the token, which contains no actual cardholder data, merchants can bill a card-on-file and schedule automatic payments. Retailers can perform data analytics, identify consumer behavior patterns, or enable omni-commerce, such as buying online and returning in store, without having to reacquire the customer's credit card number.

Tokenization helps to ensure that if an attacker does get into their environment, there's nothing that attacker can do with that data. Because it is tokenized data it cannot be monetized and sold on the dark web. It mitigates and devalues that data to ensure that attackers can't benefit from the breach.

Merchants know they need to perform full risk assessment but often don't know where to start. One resource is the National Institutes of Standards and Technology (NIST) cybersecurity framework. NIST is a great asset for organizations to understand how to assess and determine their own risk.

AI IS CREATING A SAFER ECOSYSTEM

Retailers are using Artificial Intelligence (AI) to help connect the dots required to protect their businesses from fraud and on the timeline that eCommerce demands. AI is increasingly important so that retailers can strike the right balance of stopping the fraudulent transactions while letting the good ones through.

Fraud detection traditionally used rules and configurations to work. If rules don't mitigate the risk, you tweak the rules and change configurations. It's somewhat of a manual process that uses real resources to make determinations and assess vulnerabilities.

AI helps identify and respond to threats with greater precision and speed than with traditional rules and configuration implementations. Machine learning and AI make it easier for merchants to identify, understand, and respond faster to protect against fraud. AI makes a lot of that learning and preservation of data easier and more efficient.

Artificial intelligence is an exciting field with seemingly limitless potential. Machine learning and AI embody the concept of continuous improvement, iterative cycles of intelligence, learning and interpretation. In the short term it's likely that it'll get stronger and smarter over time helping to combat a variety of susceptibilities that come with data storage and processing.

TAKING A CLEAR-EYED VIEW TO FUTURE THREATS

There is no vertical that's more or less vulnerable in terms of attacks. All industries should be on high alert. It doesn't matter if you're a small merchant, mid-market or national chain. With everything becoming more connected, it's likely we'll start to see attacks exploiting new vulnerabilities. The sophistication of bot attacks will expand to smart consumer devices in addition to enterprise infrastructure.

When working with third parties, retailers should look at their security requirements and build an effective plan to manage risk. Ultimately, it's up to each organization to be proactive as part of their assessments and not just setting a contract and walking away.

If you're doing retail transactions where you're capturing payment data, use encryption for all retail transactions. It has been proven to reduce and thwart an attack. If you're storing cardholder data—as many larger enterprise and mobile commerce merchants do—use tokenization. Not all tokenization is created equal, so insure the service providers you're using can demonstrate practical current expertise at scale without impacting your ability to provide excellent customer service.

Implementing data protection technologies like encryption and tokenization is necessary but not sufficient to protect customer data. Being confident that those solutions are operating as expected is also needed so make sure your solution also provides alerts to help you identify when there's a problem. Finally, all retailers should have a documented incident response plan so that you can take quick and effective action as needed.

MAKING DATA PROTECTION MISSION CRITICAL

Retailers face both real and perceived threats that make protecting customer data mission critical. The material costs of a data breach are well documented and retailers need to understand those risks and plan for their mitigation. If there's a perceived security threat, customers will go elsewhere. Customers will abandon their cart and their loyalty if they feel like they're not safe and secure.

Ultimately a layered approach represents best practice for any organization seeking to protect customer data. You have a house key to get in your door—but you probably also have an alarm and a smoke detector. Those are different tools designed for different attack vectors or threats in your house.

That same layered approach is essential in preparing an effective defense of your company's vital assets, including the customer data you're responsible for protecting. Retail organizations face a myriad of threats from a variety of attackers using diverse tools in heterogeneous environments. The importance of protecting customer data makes investments in layered defenses an essential pillar for any retailer security plan.

worldpay
from FIS

WFEN015 01.20