JUNE 2021

DIGITAL SECURITY

PLAYBOOK

Building Trust And Loyalty Online

The Digital Security Playbook: Building Trust And Loyalty Online, a PYMNTS and Sift collaboration, is based on a survey of 2,563 United States consumers. It examines the trust signals that inform consumers' retailer choices and offers merchants insights on how to leverage digital trust to stoke customer engagement.

DIGITAL SECURITY PLAYBOOK

Building Trust And Loyalty Online

TABLE OF CONTENTS

PYMNTS.com | sift

The Digital Security Playbook: Building Trust And Loyalty Online was done
in collaboration with Sift, and PYMNTS is grateful for the company's support and insight.
PYMNTS.com retains full editorial control over the following findings, methodology and data analysis.

INTRODUCTION

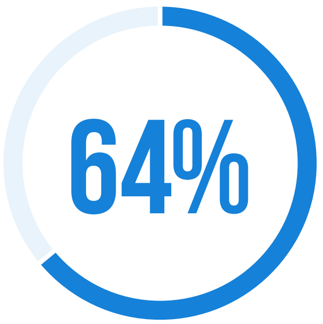
Digital trust — consumers' sense of security online — has become a primary factor driving retailer and shopping channel choice. Recent research by PYMNTS shows that consumers across all demographics feel the most secure when shopping with retailers they trust to protect their personal information.

In The Digital Security Playbook: Building Trust And Loyalty Online, we will examine the trust signals that inform consumers' retailer choices and offer merchants insights on how to leverage digital trust to stoke customer engagement.

THE NEW MOBILE BENCHMARK:

Why mobile shopping habits make digital trust paramount for retailers

Sixty-four percent of millennials use mobile devices to shop with merchants for the first time.



Most consumers now use their mobile devices to shop online with their favorite merchants or discover new "big box" eCommerce sellers. Mobile shopping adoption numbers are exceptionally high among millennials and bridge millennials, who represent some of the most engaged and frequent online shoppers. Approximately 75 percent of millennials and 72 percent of bridge millennials use their mobile devices to shop with retailers where they are regular customers, and they use mobile devices to discover new merchants online 64 percent and 63 percent of the time, respectively.

This mobile shift has brought data security concerns to light for consumers and retailers. Mobile fraud attempts rose in 2020, according to the FCC, and retailers were confronted with the need to rapidly transform their approach to protecting consumers' data as demand for mobile shopping experiences grew.[1] Heightened exposure to potential risk likely fueled consumers' overwhelming concerns about their data security and made shopping with retailers who were perceived as trustworthy even more appealing. PYMNTS' research indicates that trust in a merchant is the most crucial determinant of retailer choice for consumers of every demographic, ranked even above a user-friendly website and recommendations from friends and family. The importance of digital trust for merchant success creates a new benchmark for mobile eCommerce. Retailers must learn how to signal trustworthiness to consumers by delivering a seamless customer experience that does not compromise strong security. Understanding the relationship between consumers' data security and their perception of merchant trustworthiness is key to inspiring and sustaining their engagement online. Consumers who trust their merchants are less concerned with the safety of their data because they believe their chosen retailer will protect their information and resolve any problems that might arise.

A recent survey of adult consumers by PYMNTS, done in collaboration with Sift, revealed that the majority of consumers agreed with the statement "Merchants should do whatever they can to protect my data." Eighty-four percent of first-time shoppers with smaller merchants were concerned with data security. This suggests that because consumers are now using their mobile devices more to shop, retailers will need to keep consumer data well-protected and make shoppers aware that they are taking steps to keep information secure.

Mobile security risks that consumers face range from identity theft "phishing" schemes to data compromises through

[1] Weber, P. Mobile Phone Texts: Spam and Scams. Federal Communications Commission. 2020. https://www.fcc.gov/news-events/blog/2020/03/02/mobile-phone-texts-spam-and-scams. Accessed June 2021.

insecure apps. Companies seeking to ensure that consumers enjoy seamless experiences must balance the need for consistent performance with robust security practices.

Retailers can ensure that consumers feel safe shopping online via mobile devices by using tools or working with a fraud prevention partner that proactively protects consumers at every touch point. Retailers evaluating their security strategy should ask themselves:

- **Does our company's approach to security focus on eliminating fraud vulnerabilities?**

  A legacy approach to security will typically direct resources toward responding to evidence of fraud attacks, but this is a costly and time-intensive approach. Developing a policy that proactively protects consumers prevents fraud attempts that may slow or interrupt the customer experience.

- **Are we able to identify and address specific fraud vulnerabilities and potential threats efficiently?**

  Fraud prevention is more than a critical fiscal strategy; it is an essential step in establishing digital trust with consumers, a key component of long-term customer engagement. Retailers should choose a fraud prevention platform or partner with specific expertise in the vast array of fraud attacks retailers may face, which can include synthetic ID-based attacks and bot-driven account takeovers (ATOs).

- **Can our company consistently provide the kinds of secure customer experiences that inspire digital trust across all devices?**

  Security and product performance are dependent variables. Consumers will not follow user authentication steps that are slow, unclear or poorly designed, but they also want to trust their retailers. Our research shows that most consumers want retailers to do everything they can to ensure that their data is safe. Look for a fraud prevention system or partner that integrates highly accurate automated fraud detection tools with proactive fraud-blocking features that do not interrupt performance.

If your organization's answer is "No" to any of these questions, it is likely time for it to reevaluate its approach to security.

SMALLER MERCHANTS may face a few extra hurdles in gaining consumer trust, according to recent research. Consumers tend to trust retailers and brands they recognize, and larger merchants are likely to have had greater exposure in the marketplace via advertising and word-of-mouth.

Here are some points to remember for small merchants wishing to increase security and product performance while inspiring greater consumer trust:

- It is critical for smaller businesses to understand their specific vulnerabilities with respect to content fraud, ranging from fraudulent user review posts with links to "phishing" sites to ATOs caused by poor data hygiene during user account creation.
- Smaller merchants should not hesitate to develop a strong security model. They are often considered the "low-hanging fruit" for fraudsters, offering abundant opportunities to steal customer data. This information is often resold, resulting in new fraud attacks and leading to data insecurity at scale for the targeted merchant. A single data breach may lead to a high volume of targeted attacks.
- Smaller merchants may not have the human resources to manually screen and review fraud vulnerabilities, but the right fraud prevention platform can block attacks by automating data security measures and limiting vulnerabilities in transaction management at checkout.

LARGE MERCHANTS may possess greater technical and human resources to help fight fraud, but they are also the more obvious targets for sophisticated criminal organizations seeking to compromise consumer data at scale and conduct repeat fraud attacks.

Here are some facts for large retailers to consider when developing a security strategy:

- Fraud attacks have been on the rise, with criminals frequently taking advantage of card-not-present schemes such as buy online, pickup in store shopping options, which often do not require a further user or identity authentication beyond the initial payment. Fraudsters use stolen credentials to quickly purchase and pick up resellable products while gaining valuable user data that can later be resold online.
- False declines can be just as costly as refunds made due to unauthorized purchases. Security measures should be intuitive, data-driven and capable of blocking malicious transactions without compromising the customer experience.
- Large retailers should be aware of the importance of consistent user and payment authentication processes for each shopping channel and utilize a security platform or tools to recognize legitimate purchasers and block fraudulent ones without interrupting the customer experience.

HOW SERIOUS IS THE ONLINE RETAIL FRAUD PROBLEM?

- **CREDENTIAL AND DATA THEFT IS EASIER THAN IT SHOULD BE TODAY.**

  Criminals can purchase access to sensitive consumer data, including login credentials to online bank accounts, for as little as $40 on the dark web.[2] Fraudsters leverage various methods, ranging from paying with cryptocurrencies to using fraudulent IDs on mobile payment apps, to sell and resell consumer data to criminals for pennies on the dollar in minutes — often well before consumers realize that their information has been compromised. It is no surprise that with such a low barrier to ATO theft, online fraud has become increasingly rampant, with networks of criminals using stolen credentials to commit fraud on a massive scale.

[2] Machine Learning Switches On To Illuminate The Dark Web. PYMNTS.com. 2021. https://www.pymnts.com/news/security-and-risk/2021/machine-learning-switches-on-to-illuminate-the-dark-web/. Accessed June 2021.

- **FRAUD ATTACKS ARE COSTING RETAILERS AND CONSUMERS MORE YEAR OVER YEAR.**

  The average eCommerce storefront faced 344 fraud attacks per year in 2020, up by 24 percent over 2019, with large retailers experiencing a 37 percent increase in fraud attacks in 2020.[3] The fiscal impact of fraud is exorbitant and rising. One recent survey suggested that for every dollar lost to fraud, an organization's total financial loss totaled $3.36 (up from $2.40 in 2016), due to various associated costs to the retailer after a successful fraud attack.[4] The FTC received more than 2.1 million fraud complaints from consumers in 2020, with consumer losses totaling $3.3 billion, up from $1.8 billion in 2019.[5]

- **DATA SECURITY IS A CUSTOMER LOYALTY PROBLEM, TOO.**

  While each eCommerce retailer may face unique security threats, consumers want seamless and secure customer experiences regardless of the challenges facing that brand. A recent survey revealed that more than half of consumers said they would not patronize an online retailer again if they experienced an incidence of fraud.[6]

[3] Deep Dive: Why eCommerce Merchants Struggle To Find A Fraud Detection Balance. PYMNTS.com. 2021. https://www.pymnts.com/fraud-prevention/2021/ecommerce-fraud-detection/. Accessed June 2021.

[4] Deep Dive: Why eCommerce Merchants Struggle To Find A Fraud Detection Balance. PYMNTS.com. 2021. https://www.pymnts.com/fraud-prevention/2021/ecommerce-fraud-detection/.Accessed June 2021.

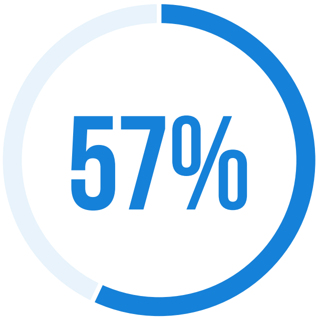
[5] FTC 2020 Data Shows Consumer Fraud Hit 2.2 Million. PYMNTS.com. 2021. https://www.pymnts.com/news/security-and-risk/2021/ftc-2020-data-shows-consumer-fraud-hit-2-2-million/. Accessed June 2021.

[6] Deep Dive: Why eCommerce Merchants Struggle To Find A Fraud Detection Balance. PYMNTS.com. 2021. https://www.pymnts.com/fraud-prevention/2021/ecommerce-fraud-detection/. Accessed June 2021.

THE DIGITAL TRUST QUICK-START GUIDE FOR MERCHANTS:

Learning how consumers shop and develop brand trust

Consumers are loyal to their favorite online retailers, but most are open to new sellers. Recent PYMNTS research reveals that although 95 percent of consumers have one or more merchants with whom they shop regularly, 57 percent have tried a new merchant within the last 12 months. Our research also shows that consumers tend to spend more at new merchants on average, as they spent $120 with them versus $95 at their usual online retailers.



Fifty-seven percent of consumers have tried a new merchant in the last 12 months.

Consumers' assessment of digital trustworthiness is a crucial driver of merchant choice, so newer and/or smaller merchants have an opportunity to engage new customers by creating a shopping environment that signals data security as an integral part of the customer experience. The following are some guidelines for merchants of every size interested in inspiring consumer engagement:

LEVERAGE CONSUMER TOLERANCE FOR "POSITIVE FRICTION" AT CHECKOUT WHEN IT CONTRIBUTES TO IMPLEMENTING DATA SECURITY MEASURES.

PYMNTS' research shows that 84 percent of consumers want small merchants to "do whatever they can" to protect their data, even if it adds time at checkout.[7] That means consumers will likely not flinch if asked to participate in a user authentication process, though they will want that "cost" to render an explicit, ongoing value such as solid data protection throughout their current and future shopping experiences.

SIGNAL TRUSTWORTHINESS BY FOCUSING ON TRANSPARENCY.

Consumers notably cited clear product descriptions (14 percent) and visible security logos at checkout (10 percent) as essential features for new small merchants to provide. Transparency for consumers means clarity about the steps a merchant is taking to protect their data and streamline the shopping experience, including everything from user-friendly product and service descriptions to the security measures designed to keep their data safe. How consumers assess the trustworthiness of a merchant appears to be related to familiarity, repeated positive experiences and the size of the retailer. Larger merchants tend to be considered more trustworthy than smaller sellers, meaning that smaller merchants should establish trust with new customers at the beginning of the shopping journey.

[7] NEW REPORT: How Online Merchants Build Trust With First-Time Customers. PYMNTS.com. 2021. https://www.pymnts.com/commerce/2021/how-online-merchants-build-trust-with-first-time-customers/. Accessed June 2021.

LARGER MERCHANTS — EVEN THOSE WITH A SIZABLE, HIGHLY ENGAGED CUSTOMER BASE — SHOULD ENSURE THAT DATA PROTECTION EFFORTS ARE STRONG WITHOUT DAMAGING THE CUSTOMER EXPERIENCE.

Our research indicates that while consumers want data security, they do not want unnecessary friction added to their experiences when shopping with large merchants they know and trust.[8] Building customer experiences that blend intuitive shopping features with solid security is key to establishing the digital trust that builds customer loyalty. PYMNTS' research shows that affluent consumers (those earning more than $100,000 per year) and baby boomer and senior consumers are highly concerned about data protection with the merchants they frequent (80 percent and 87 percent, respectively), yet a frictionless customer experience is still a high priority.[9] Consumers are less concerned with data security when shopping with trustworthy merchants, especially large retailers with whom they have shopped before. That makes the customer experience even more critical for large merchants with a loyal audience of consumers.

CHOOSE THE RIGHT FRAUD PROTECTION PLATFORM OR SERVICE.

Choosing the right service or platform to manage your fraud-blocking efforts is essential. An outdated approach to security may block legitimate consumer traffic, resulting in costly false declines, which compromise customer experience and alienate users. An inconsistent security approach may be sufficient on some devices but fail at scale. Look for a provider that automates fraud blocking and prevention using AI-based modeling of the range of legitimate customer behaviors. This allows retailers to automatically block fraudulent behaviors while limiting false declines.

[8] Checkout Conversion Index. January 2021. PYMNTS.com. https://securecdn.pymnts.com/wp-content/uploads/2021/01/2021-01-Index-Checkout-Conversion-Index-Report.pdf. Accessed June 2021.

[9] NEW REPORT: How Online Merchants Build Trust With First-Time Customers. PYMNTS.com. 2021. https://www.pymnts.com/commerce/2021/how-online-merchants-build-trust-with-first-time-customers/. Accessed June 2021.

4 TYPES OF DATA TO LOOK FOR FROM YOUR FRAUD PREVENTION SERVICE:

RETAILER-SPECIFIC:
The retailer's data

REGIONAL-SPECIFIC:
Data from retailers in the same region

INDUSTRY-SPECIFIC:
Data from retailers in the same retail industry

UNIVERSAL:
Data from all retailers using the service or platform

The correct data will optimize fraud-blocking efforts and inform more accurate future security. Look for a vendor that provides this data in the context of potential fraud vulnerabilities, customer behaviors and real-time insights based on how specific customer groups shop and interact with your website, apps or other digital properties.

CONCLUSION

Retailers face a mounting range of complex security challenges. eCommerce companies must address known vulnerabilities to fraud attacks while not interrupting a positive customer experience. Leveraging digital trust by improving customer experience along with creating strong data security can enhance customer engagement for leading retailers and bring new audiences to emerging online merchants.

READ MORE ON

MAY 2021

THE TRUST QUOTIENT

How Merchant Trust Drives Shopping Behaviors

PYMNTS.com sift

The Trust Quotient

MAY 2021

How Online Merchants Build Trust With First-Time Customers

Keeping data protection front and center can help merchants put first-time customers at ease — and keep them coming back. In The Trust Quotient: How Merchant Trust Drives Shopping Behaviors, PYMNTS surveys 2,563 U.S. consumers to better understand what visual cues consumers seek and need to build trust when deciding to check out with a merchant they have never shopped with before.

DIGITAL SECURITY PLAYBOOK

Building Trust And Loyalty Online

ABOUT

PYMNTS.com is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

Sift is the leader in Digital Trust & Safety, empowering digital disruptors to Fortune 500 companies to unlock new revenue without risk. Sift dynamically prevents fraud and abuse through industry-leading technology and expertise, an unrivaled global data network of 70 billion events per month and a commitment to long-term customer partnerships. Global brands such as Twitter, Airbnb and Twilio rely on Sift to gain competitive advantage in their markets. Visit us at sift.com and follow us on Twitter @GetSift.

We are interested in your feedback on this report. If you have questions, comments or would like to subscribe, please email us at feedback@pymnts.com.

DISCLAIMER

The Digital Security Playbook: Building Trust And Loyalty Online may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS.COM: MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS.COM SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS.COM RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS.COM SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS.COM AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.