CONSENT MANAGEMENT:
CUSTOMERS TAKE CONTROL

Financial Services

CONSENT MANAGEMENT:
CUSTOMERS TAKE CONTROL

When the digital marketing era began, customer data quickly became a gold mine for marketing professionals, including those in the financial services industry. As they gathered more and more data, those professionals developed ever-deeper insights that let them reach customers with increasing effectiveness.

Customers typically saw this as a good deal — for a while, at least. Financial services companies' use of data often meant convenience and a better consumer experience as companies created relevant, personalized interactions. In general, consumers were willing to provide their personal information without conditions.

In time, consumers began to see potential downsides to sharing their data. Concerns about large data breaches and identify theft increased. At times, "too targeted" advertisements felt overly intrusive. Eventually, consumers considered sharing their data as a risk and became increasingly protective of their personal information making data privacy a high-profile issue.

In a survey conducted in 2020 by DataGrail, 83% of respondents said they want to have control over how businesses use their data, and 54% said they were "either fed up, frustrated, or creeped out by companies that use their data to serve targeted, personalized ads.[1]" Such sentiments have been gaining traction with governments, leading to a growing number of laws that give consumers more rights when it comes to the collection and use of their personal information.

These trends are putting a spotlight on consent management — the process of getting customers' permission to use their personal information. As financial services customers gain more control over their data, consent management will be critical to acquiring the raw material for effective data marketing. This will be key to limiting compliance risk, strengthening relationships with customers, and remaining competitive as the rules and attitudes around data privacy continue to evolve.

[1] DataGrail,"DataGrail's 2020 Consumer Privacy Expectations Report," 2020.

THE SHIFTING CONSENT LANDSCAPE

In recent years, a number of new and often stringent laws and regulations have appeared around the globe. Among the most significant of these are the European Union's (EU) General Data Protection Regulation (GDPR) and its ePrivacy Directive. To comply with these requirements, companies must have individuals "opt in" and actively agree to the collection of their data. Under GDPR, consent means that this agreement is "freely given, specific, informed, and unambiguous."

Warnings and checkboxes simply asking for consent are not enough. The ePrivacy Directive mandates that companies owning and managing websites and applications with cookies and similar tracking technologies provide a mechanism for users to opt in or out of optional cookies. Fines for noncompliance with these regulations can be severe. For example, fines for GDPR violations can be as much as €20 million or 4% of a company's worldwide revenue — whichever is higher. In addition, the EU's proposed ePrivacy Regulation 2021 would build upon the ePrivacy Directive and expand its definitions.

A number of other countries, including Canada, South Africa, New Zealand, and Brazil, have followed suit with data privacy laws of their own. In the U.S., however, there is no overarching federal data privacy law. Instead, the issue is addressed at the state level.

Following the lead of the GDPR, California passed its own California Consumer Privacy Act (CCPA), which took effect in 2020. While not as strict as the EU law when it comes to consent, the act gives consumers the right to know what personal information is being collected and who it's being sold to, the ability to have their personal information deleted, and to opt out of the sale of their personal information. It does require opt-in consent from teenage minors or, for younger children, their parents. In addition, some health and financial data that is governed

Following California's lead, other states, including Virginia and Colorado, have passed some form of data privacy law and many others are considering it. California further strengthened its privacy laws by recently passing the California Privacy Right Act, which goes into effect in 2023. This act expands some of the consumer rights in the CCPA, allows consumers to sue companies for non-compliance, and sets up a new state agency to enforce the law.

In short, data privacy involves an evolving and complicated patchwork of laws that vary from jurisdiction to jurisdiction. But the bottom line is clear, governments are focusing on giving more control to consumers when it comes to personal information and that begins with gaining their permission to collect and use that data.

In addition to these legal and regulatory requirements, marketing professionals need to adjust to changes taking place in the private sector. In response to privacy concerns, a number of browsers are limiting the use of third-party cookies — a key tool that lets companies track consumers across web sites to personalize offers, track marketing campaigns, and so forth. Over the last two years, the Safari and Firefox web browsers have started to block third-party cookies by default and Apple is adding privacy features to its iPhone that require users to opt in if they want companies to track their web activity. Google, which has a two-thirds share of the global browser market,[2] plans to block third-party cookies by the end of 2023.

These changes mean that financial services companies will need to rely more heavily on data gathered with customers' consent, such as the first-party cookies that companies use on their own sites to identify consumers.

Overall, the need to gain customers' consent to use their data is growing more important and more complex — all of which requires increasing sophistication in consent management processes.

[2] Statcounter GlobalStats, "Desktop Browser Market Share Worldwide - January 2022."

CONSENT MANAGEMENT FOR THE FUTURE

At heart, financial services companies need to take a more centralized approach to consent management. This begins with technology and a consent management platform that offers a full range of consent management capabilities. There are a number of such platforms available on the market, but ideally, the platform should integrate consent management with the systems used to collect and process customer data. It should enable companies to offer each customer the appropriate consent options, manage consent for each customer across platforms and marketing contact points, give the customer transparency into the data being collected and used, and log and track consent for compliance.

"Financial services institutions have to comply with a variety of customer privacy protection regulations such as GDPR, the ePrivacy Directive, and CPRA, while working with customers through many communication channels," says Alok Benjwal, Vice President, Financial Services, at Capgemini. "That means that they need to have a central repository of privacy and customer preference data that can be used by the entire institution. It also means that they need to enable customers to easily manage their own privacy options and preferences across channels and product relationships. A consent management platform will allow them to seamlessly communicate with customers without infringing on customer preferences for how their data is used."

As companies put consent management platforms in place, there are several key questions they should consider to help them make the most of the technology.

How will our organization's compliance and regulatory roles need to change to manage this capability?

The implementation of this platform should be based on a broader consent management strategy that considers the company's industry, business model, size, brand complexity, and the laws and regulations in the places where it operates. The strategy should incorporate organizational changes as well. Financial services companies need to define consent management roles and align consumer data privacy requirements with their compliance and data governance groups. They should also charge the Chief Data Officer, or another executive, with overseeing consent management — not only for marketing purposes, but to ensure that consent practices remain in compliance with the law as well.

How can we incentivize customers to share their data in return for clearly understood value?

Financial services companies should rethink their larger content strategy and their brand value through the lens of consent-based marketing. This will allow them to create experiences in which the customer clearly understands the value of sharing their data with the company, and how they will benefit from it. Making this case and gaining consent for first-party cookies will be especially important as third-party cookies are phased out.

How will consent management factor into our brand's customer data management and data governance processes?

Preparing a company's data for effective consent management can be particularly challenging. Financial services companies often lack a central customer data pool leading to poor data quality, a lack of transparency into the status of consent, and challenges in scaling up consent management to work throughout the enterprise. There may also be varied approaches to consent across business units and regions making it difficult to ensure compliance in all jurisdictions.

Solving these data-related problems can pay off in better consent management. For example, when Capgemini analyzed one company's data landscape, it found that the customer data quality was unreliable due to a lack of centralized customer data and the company's use of multiple consent management systems in different European countries. Capgemini worked with the company to build a uniform, standardized consent management system for the whole company. This included the creation of a centralized customer data pool, the implementation of better data sharing throughout the company and its ecosystem of partners, and a more robust data protection standard throughout its European operations. As a result, the company had a single point of truth for consent information about its customers on all sales levels with the ability to perform personalized, data-driven lead and campaign management — while being compliant with the GDPR.

A COMPETITIVE EDGE

Through effective consent management, financial services companies can avoid fines and the reputational damage of noncompliance in the evolving data privacy world. When approached correctly, it can help them avoid risk and compete more effectively.

Consent management is an increasingly vital capability for successful data marketing; it lays a foundation for everything from effective omnichannel strategies to profiling and marketing automation. What's more, consumers today value companies that they can trust — those they see as ethical and acting with transparency and purpose. Often, they see this as more important than traditional factors such as price and quality.

Financial services companies can turn what many see as a compliance exercise into a competitive differentiator. They can use consent management to demonstrate that they are trusted stewards of personal data and they can put themselves in a position to acquire more customers, increase customer loyalty, and build brands that consumers trust.

FOR MORE INFORMATION, PLEASE CONTACT:

Ashvin Parmar
VP & Global Leader, Solutions
Financial Services Insights & Data
ashvin.parmar@capgemini.com

Kevin Farley
Marketing Analytics Leader
Financial Services Insights & Data
kevin.farley@capgemini.com

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 325,000 team members more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2021 global revenues of €18 billion.

CONTACT US AT

financialservices@capgemini.com