KB

INTEGRATING IDENTITY AND PRIVACY WITH DIGITAL CUSTOMER EXPERIENCE: TURNING NEGATIVES INTO POSITIVES

November 2021

Derek E. Brink, CISSP
Vice President and Research Fellow, Cybersecurity and IT GRC

ABERDEEN
STRATEGY & RESEARCH
ILLUMINATE. INSPIRE. IGNITE.

Executive Summary

When it comes to managing identity and privacy in consumer-facing online businesses, friction in the customer experience can quickly lead to failures in the achievement of strategic business outcomes — not to mention the downside risks and costs related to cybersecurity and regulatory compliance. Integrating solutions for CIAM and ECPM in the broader context of proactively managing digital customer experiences can help to transform these negatives into positives.

Integrating Identity, Privacy with Customer Experience

Consumer-facing online businesses typically have well-defined business objectives for *customer / subscriber acquisition and retention*, *revenue and profitability growth*, *market share*, and so on. These **strategic business outcomes** are driven in large part by how effectively online customers can move through the experience of visiting websites and other digital properties, actively engaging with products and services of interest, and ultimately making purchases — a process which organizations commonly measure and manage using **key performance indicators (KPIs)** such as *bounce rate*, *add to cart rate*, *cart abandonment rate*, *conversion rate*, and *average order value*.

Integrating solutions for **Customer Identity and Access Management (CIAM)** and **Enterprise Consent and Preference Management (ECPM)** into the broader context of proactively managing digital customer experiences can be a highly effective way for consumer-facing, online businesses to transform negatives into positives.

Unfortunately, to the extent that current **customer identity** and **data privacy consent / preference management** experiences contribute to *higher abandonment rates* and *lower conversion rates* for day-to-day transactions — and ultimately to *lower retention rates* for ongoing account-based relationships — they can have a significant negative effect on the organization's achievement of the desired business outcomes. In this context, friction in the customer experience can quickly lead to failure.

Conversely, however, investments in personalized and friction-free customer experiences related to identity and data privacy can lead to quantifiable *improvements* in these key performance indicators, making a financially material contribution to the achievement of strategic business outcomes. At the same time, these investments can also have the added benefit of helping to address growing **cybersecurity risks related to digital identities** (e.g., *credential stuffing*, *account takeovers*, *fraud*) and expanding **regulatory compliance requirements related to data privacy and consent** (e.g., *GDPR*, *CCPA*, *LGPD*).

Said another way: Integrating solutions for **Customer Identity and Access Management (CIAM)** and **Enterprise Consent and Preference Management (ECPM)** into the broader context of proactively managing

digital customer experiences can be a highly effective way for consumer-facing online businesses to turn these negatives into positives. See Table 1.

Table 1: Integrating Identity and Privacy into the Broader Context of Proactively Managing Digital Customer Experiences Can Turn Negatives into Positives

Negatives that are addressed by Customer Identity and Access Management (CIAM)	Negatives that are addressed by Enterprise Consent and Preference Management (ECPM)	Positives for Consumer-Facing Online Businesses
Key Performance Indicators: • Higher abandonment rates • Lower conversion rates • Lower retention rates	Key Performance Indicators: • Higher abandonment rates • Lower conversion rates • Lower retention rates	**Improve KPIs** **Achieve Strategic Business Outcomes** **Enable Upside Opportunities**
Strategic Business Outcomes: • Lower revenue • Higher costs • Lower customer trust and loyalty	Strategic Business Outcomes: • Lower revenue • Higher costs • Lower customer trust and loyalty	
Growing cybersecurity risks related to digital identities (e.g., *credential stuffing*, *account takeovers*, *fraud*)	Expanding regulatory compliance requirements related to data privacy and consent (e.g., *GDPR*, *CCPA*, *LGPD*)	**Reduce Downside Risks** **Sustain Regulatory Compliance**
Total cost of data breaches, total cost of identity-related fraud	Total cost of regulatory fines and judgments	

Source: Aberdeen, November 2021

To illustrate: Aberdeen conducted phone-based interviews with subject-matter experts in each of six selected eCommerce retail categories, from which a range of performance for selected KPIs in each category could be established. The results are shown in Table 2.

Table 2: eCommerce Funnel KPIs — Research Findings / Modeling Parameters

eCommerce Category	Bounce Rate			Add to Cart Rate			Cart Abandonment Rate			Conversion Rate			Average Order Value		
	low	most likely	high	low	most likely	high	low	most likely	high	low	most likely	high	low	most likely	high
All Categories	38.0%	**56.9%**	77.0%	5.4%	**7.8%**	12.0%	46.0%	**63.3%**	80.4%	1.25%	**2.37%**	4.20%	$28	**$202**	$800
Consumer electronics	42.8%	46.9%	53.5%	7.4%	8.4%	10.0%	62.0%	69.2%	80.4%	1.70%	2.20%	2.60%	$150	$246	$400
Fashion and beauty	55.0%	64.7%	77.0%	5.5%	6.4%	7.4%	55.0%	64.3%	74.0%	1.25%	1.90%	2.50%	$80	$270	$800
Food and beverage	48.0%	51.7%	56.0%	8.8%	10.5%	12.0%	52.0%	59.9%	65.0%	2.80%	3.44%	4.20%	$48	$61	$86
Furniture, Appliances, and Home Improvement	65.0%	70.0%	74.5%	5.4%	6.7%	8.0%	55.0%	61.8%	74.0%	1.60%	2.28%	3.20%	$216	$320	$460
General merchandise	38.0%	48.9%	57.0%	7.0%	8.8%	11.0%	46.0%	61.3%	70.0%	1.80%	2.56%	3.60%	$85	$145	$250
Health and Leisure	46.0%	52.2%	60.0%	5.8%	7.3%	10.0%	56.0%	63.6%	78.0%	1.60%	2.00%	2.40%	$45	$165	$238

Research findings represent the range (90% confidence interval) and most likely value for each KPI, expressed as a percentage of total visitors (total visitors = 100%). Source: Aberdeen, November 2021

Using quantitative models, it's reasonably straightforward to evaluate the potential to improve top-line revenue — i.e., *(number of visitors) x (conversion rate) x (average order value)* — based on estimating the incremental benefits from making investments in improving digital customer experiences related to identity (e.g., CIAM) and privacy (e.g., ECPM). These cause-and-effect relationships include:

- Greater flexibility and convenience → Growth in *total customers*
- Higher trust and loyalty → Higher *customer retention*
- Personalized customer experiences → Increased engagement; reduced *bounce rates*; higher *add to cart rates*; higher *conversion rates*
- Convenient, frictionless digital experiences across multiple properties, brands, and regions → More *transactions per customer*; higher *order value per transaction*

Over time, the cumulative impact from all of the above is reflected in higher *lifetime value per customer* and higher *total revenue* — i.e., in the achievement of the organization's strategic business outcomes.

Focus: Cybersecurity Risks Related to Digital Identities

As noted above, integrating solutions for identity and privacy in the broader context of managing digital customer experiences can also have the added benefit of helping to address growing **cybersecurity risks related to digital identities** (e.g., *credential stuffing*, *account takeovers*, *fraud*).

From the perspective of financially motivated attackers, there are three obvious reasons why **credential stuffing attacks** against consumer-facing online businesses represent such a rich opportunity:

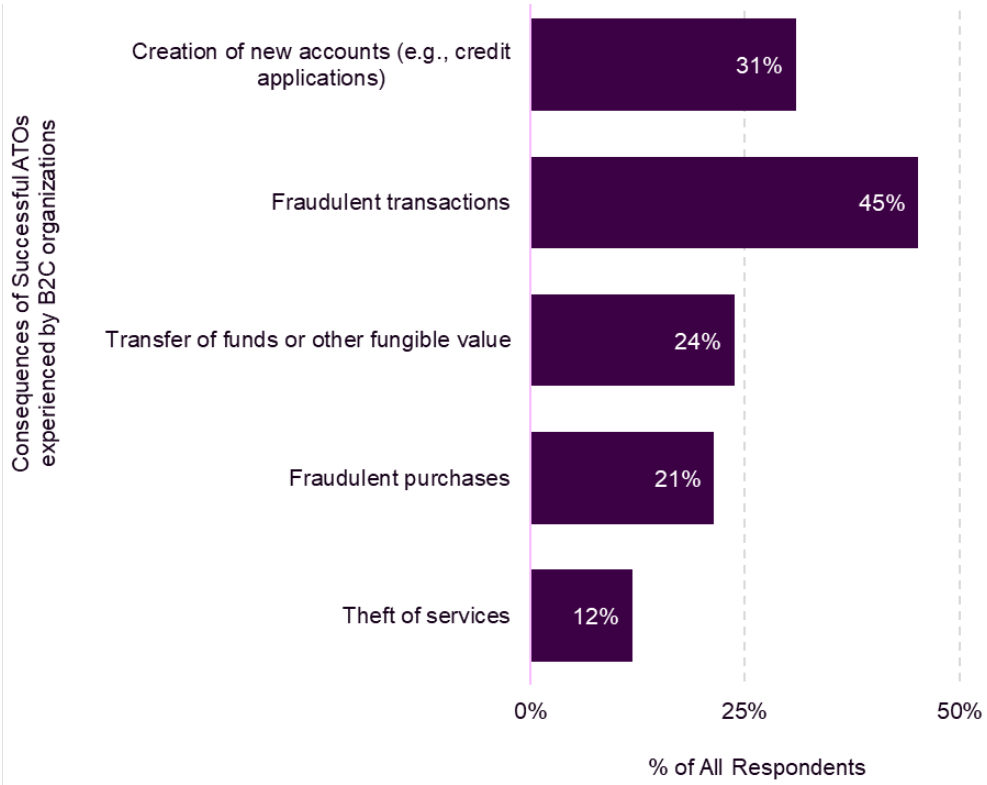
- Credential stuffing attacks are an effective, brute-force way for attackers to exploit weak or compromised digital credentials and gain unauthorized access to user accounts.
- Credential stuffing attacks have become significantly easier for attackers to automate (e.g., using bots), at Internet speed and scale.
- Financially motivated attackers are making successful **account takeovers** pay off in several ways, including *creation of new accounts* (e.g., credit applications); *fraudulent transactions*; *transfer of funds or other fungible value* (e.g., loyalty points, rewards); *fraudulent*

Credential stuffing refers to the process of automating the input of user credentials (e.g., obtained from a database of usernames and passwords that were compromised in a data breach) into the login page of a digital property, in an attempt by an unauthorized party to achieve an *account takeover*.

Account takeovers (ATOs) refer to successful access to a legitimate user's account by an unauthorized party, as a conduit to commit financial fraud.

purchases (e.g., physical goods, stored value cards); and *theft of services* (e.g., download or streaming of digital content). See Figure 1.

Figure 1: Financially Motivated Attackers Can Make Successful Account Takeovers Pay Off, in Several Ways



Source: Aberdeen, November 2021

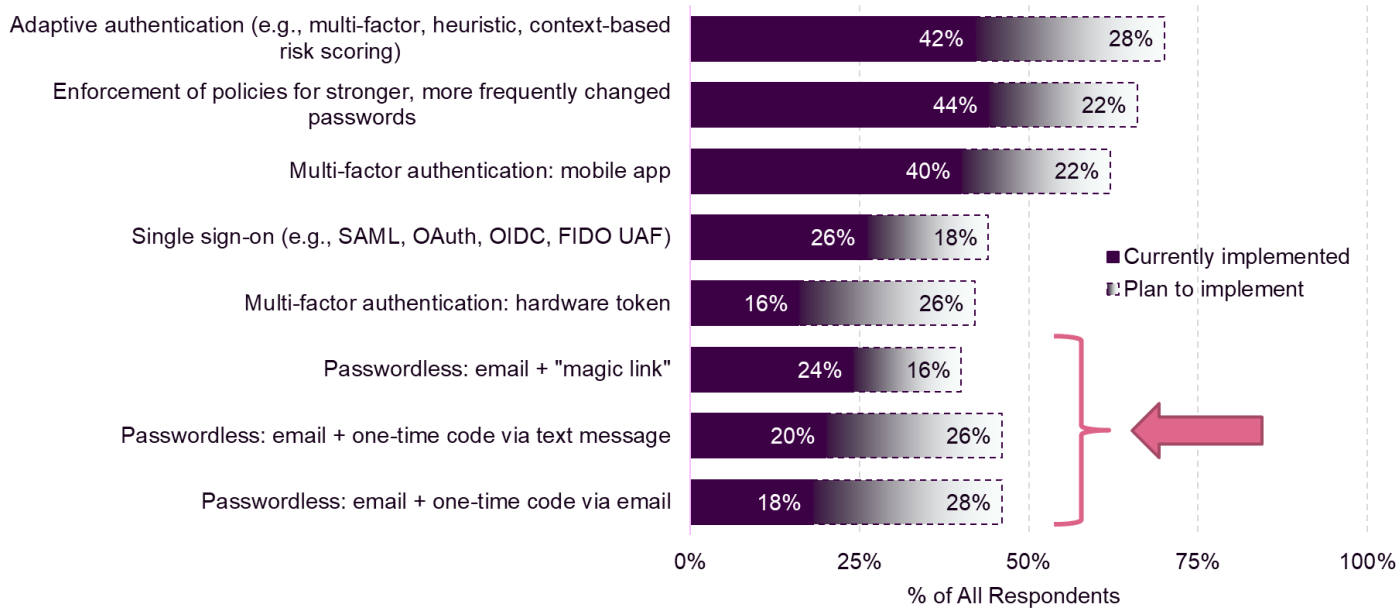
From the defender's perspective, the flip side of these same three reasons are why customer-facing online businesses are being forced to pay closer attention to credential stuffing and account takeovers:

- Digital credentials are central to the way they manage the long-term, account-based relationships with their digital customers.
- Bot-driven credential stuffing attacks are prevalent, and growing. In Aberdeen's recent research, 84% of all respondents reported that some number of their online users had experienced a successful account takeover in the previous 12 months.
- The financial consequences of successful account takeovers — both direct, and indirect — have grown beyond a basic "cost of doing business" to become a financially material business risk. In the **FinTech** category, for example, Aberdeen's analysis estimates the **direct cost of fraud from ATOs ranged from 2.6% to 7.1% (median: 4.8%)** of the revenue generated from monthly active users.

In Aberdeen's recent research, 84% of all respondents reported that some number of their online users had experienced a successful account takeover in the previous 12 months.

In response, consumer-facing online businesses have increasingly adopted a variety of technologies designed to address the weaknesses of traditional passwords, which reduces the likelihood of successful ATOs (see Figure 2). Most recently, *passwordless* approaches to user authentication have gained strong interest — and are being supported by leading providers of CIAM solutions.

Figure 2: Consumer-Facing Online Businesses Have Adopted a Variety of Technologies Designed to Address the Weaknesses of Traditional Passwords



Source: Aberdeen, November 2021

Focus: Privacy / Consent Requirements for Digital CX

Finally, integrating solutions for identity and privacy in the broader context of managing digital customer experiences can also help to address expanding **regulatory compliance requirements related to data privacy and consent** (e.g., *GDPR*, *CCPA*, *LGPD*).

Few enterprise-wide initiatives in recent memory can compare with GDPR in overall scale and scope. For example:

- The **Year 2000 (Y2K) Bug** — which drove organizations to find and remediate problems in how software programs dealt with dates beyond December 31, 1999 — was primarily a *technology* initiative.
- Variations of the **Sarbanes-Oxley Act (SOX, EuroSox, J-SOX, C-SOX)** — put in place to protect investors in the wake of fraudulent corporate accounting activities by publicly traded companies — are

predominantly about the *people and processes* related to financial controls, record-keeping, and reporting.

But data privacy and consent initiatives such as GDPR are even more comprehensive than SOX or Y2K, in the sense that they involve enterprise-wide attention to people, processes, *and* technologies. Even worse: For many customer-facing online businesses, GDPR is just one of a growing number of complex, enterprise-wide compliance requirements for data privacy and consent management that must be dealt with (see Table 3).

Aberdeen's research found that 75% of all respondents had at least one significant non-compliance issue (median: 3) over the previous 12 months.

Table 3: Data Privacy and Consent Examples (GDPR, CCPA, LGPD)

	EU General Data Protection Regulation (GDPR)	California Consumer Privacy Act (CCPA)	Brazil General Data Protection Law (LGPD)
Authority	European Union	California	Brazil
Effective date	May 25, 2018	January 1, 2020	August 15, 2020
Personal data	Any information related to the identification of a natural person, directly or indirectly	Any information which can identify, is capable of being associated with, or can reasonably be linked to a consumer household, directly or indirectly	Any information related to the identification of a natural person.
Examples	name, account numbers, social identifiers	Consumer preferences, behaviors, characteristics, behaviors	none provided
Applicability	Any entity that process personal data for the purpose of (i) offering goods or services, or (ii) monitoring the behavior of individuals located in the EU	Any for-profit business that operates in California, processes the personal data of consumers residing in California, and meets at least one of the following: (i) gross revenue of >=$25M / year, (ii) processes personal data of >50K consumers / year, (iii) derives >=50% of annual revenue from selling the personal data of California residents	Any information relating to the identification of a natural person.
Fines and Judgments	Up to €20M or 4% of total global annual revenue for the previous year, whichever is higher	$100 and $750 / consumer / incident, or actual damages, up to $7.5K for each intentional violation; no total cap	2% of gross revenue in Brazil, to a maximum of R$50M Daily fines

Source: Aberdeen, November 2021

A key point from the high-level summary in Table 3 is that the inclusion of meaningful “teeth” in data privacy and consent regulations has had a powerful effect on *executive-level attention*, and on the resulting *allocation of resources* for data privacy and consent management initiatives — which further strengthens the case for integration of solutions such as ECPM.

Summary and Key Takeaways

- For consumer-facing online businesses, investments in personalized and friction-free customer experiences related to identity and data privacy can lead to quantifiable **improvements in key performance indicators**, making a financially material contribution to the **achievement of strategic business outcomes**.
- At the same time, these investments can also have the added benefit of helping to address **growing cybersecurity risks related to digital identities** (e.g., *credential stuffing*, *account takeovers*, *fraud*) and **expanding regulatory compliance requirements related to data privacy and consent** (e.g., *GDPR*, *CCPA*, *LGPD*).
- Integrating solutions for **Customer Identity and Access Management (CIAM)** and **Enterprise Consent and Preference Management (ECPM)** into the broader context of proactively managing digital customer experiences can be a highly effective way for these businesses to transform the negatives into positives.

About Aberdeen Strategy & Research

Since 1988, Aberdeen has published research that helps businesses worldwide to improve their performance. Our analysts derive fact-based, vendor-neutral insights from a proprietary analytical framework, which identifies Best-in-Class organizations from primary research conducted with industry practitioners. The resulting research content is used by hundreds of thousands of business professionals to drive smarter decision-making and improve business strategies. In 2020, Aberdeen became part of Spiceworks Ziff Davis.