ACI Speedpay® Pulse Report

2024 ACI Speedpay® Pulse Report:

Billing and payment trends and behaviors — Focus on fraud

ACI Worldwide®

Foreword: Consumers are looking for guidance from billers on security and fraud prevention

Ron Shultz
Head of ACI Speedpay®
ACI Worldwide

Welcome to the latest edition of the ACI Speedpay® Pulse Report. The largest and longest running consumer survey of America's billing, payment, and communication preferences continues to evolve with new questions added to reflect the rapid proliferation of digital communications and payment channels, and the simultaneous increase in digital identity and payments fraud.

What have we found in the first half of 2024?

Preferences for digital payment channels are on the rise again. This is welcome news for billers when it comes to managing costs and improving the customer experience.

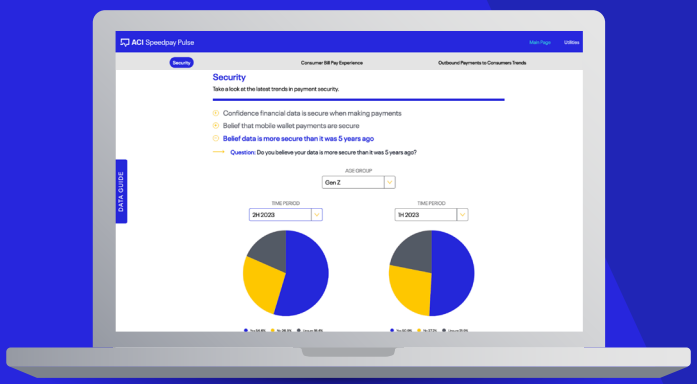
But for all the benefits of digitization in terms of convenience and control, it also opens the door to risks such as online identity theft, which our survey also shows to be relatively and persistently high.

Anecdotally, we know from conversations with customers that fraud rings are proving just as able as billers when it comes to leveraging new technology, such as artificial intelligence (AI), to automate and scale their operations. This is particularly relevant when it comes to the phishing scams that are a favored on-ramp for identity and data theft.

The impact of fraud is being keenly felt by consumers in unwelcomed losses, to say the least, while many continue to feel the financial strain of high interest rates and diminished purchasing power from persistent inflation.

The good news for billers, however, is that our survey also reveals how consumers want them to respond regarding additional account protections and educational outreach. This is exactly what the industry has come to expect from the ACI Speedpay® Pulse Report: practical advice to help billers respond to the biggest payment trends impacting their industry and their customers.

So, happy reading. As always, this report is a necessarily high-level summary of a much wider survey, which you can explore at your leisure using our interactive data exploration tool.



Data at your fingertips

As a premier authority in the billing and payments industry, ACI prides itself on keeping a pulse on the evolving needs of consumers, as well as the trends impacting the industry.

Our interactive data exploration tool is designed to let you quickly view the billing and payment preferences of thousands of consumers over several years.

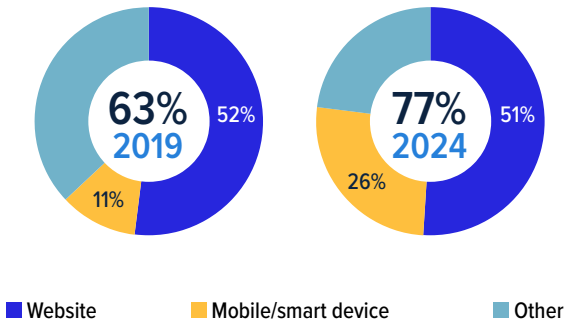
More than three quarters of Americans now prefer to pay their bills digitally

Consumer preference for paying their bills via digital channels is continuing its six-year upward trend, and more than three quarters of Americans now prefer to pay digitally (**Figure 1**). The remaining 23% prefer analog channels such as CSR-assisted or IVR phone payments, in-person payments, or paying by mail.

The shift to mobile, primarily driven by biller and bank mobile apps, plus digital wallets like Apple Pay and Google Pay, is also more pronounced than ever.

Figure 1

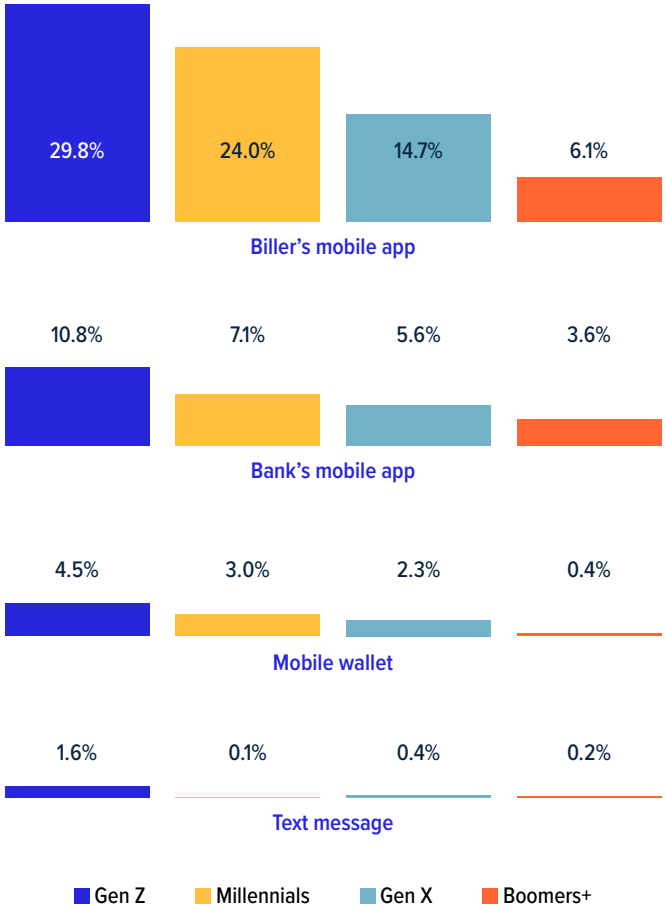
What is your preferred channel for making one-time bill payments?



As would be expected, this shift is being led by the younger generations, with Gen Z and Millennials displaying the strongest year-on-year growth in preference for mobile (**Figure 2**). However, far from being laggards, the majority of Boomers have also gone digital, albeit showing a marked preference for paying via billers' websites compared to their younger counterparts.

Figure 2

Preferred channel for making one-time bill payments by generation



Gen Z
Born after 1997

Millennials
Born 1981-1996

Gen X
Born 1965-1980

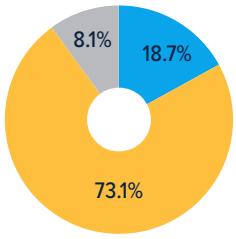
Boomers+
Born before 1965

Nearly 1 in 5 struck by online identity fraud

Almost one in five consumers (**18.7%**) report falling victim to online identity theft. Among this group, two in five report that this incident resulted in accounts being opened in their name. Most often these were credit card and/or bank/checking accounts (**Figure 3**).

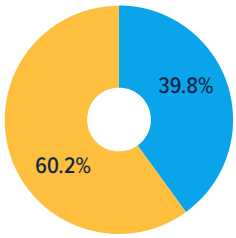
Figure 3

Have you ever been a victim of online identity theft?



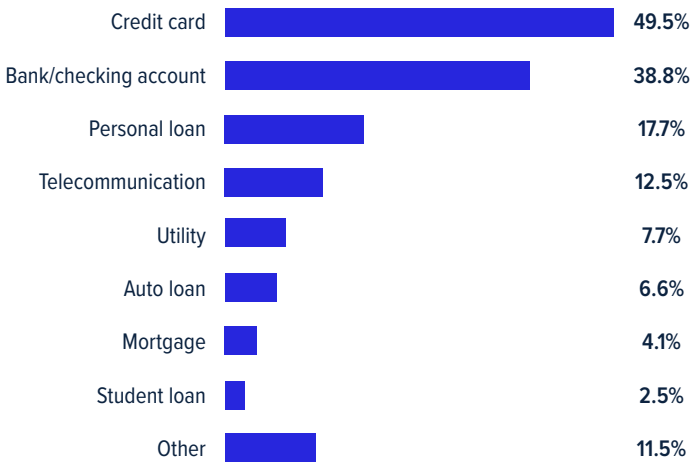
Yes No Not sure

If so, did the online identity theft involve accounts being opened up in your name?



Yes No

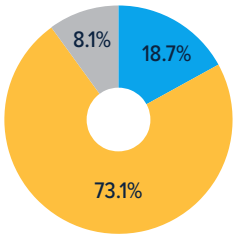
If so, what type of accounts did they open?



Continuing to look at the fallout for those consumers that fell victim to online identity theft, half said these incidents also resulted in a financial loss. For most, the loss was $1,000 or less (**Figure 4**). But any level of loss will be unwelcome in these difficult economic times and for almost a third (**31%**), it was more than $1,000. One in ten experienced losses that exceeded $5,000.

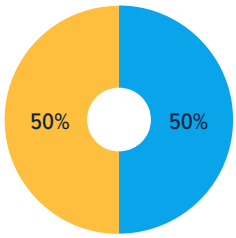
Figure 4

Have you ever been a victim of online identity theft?



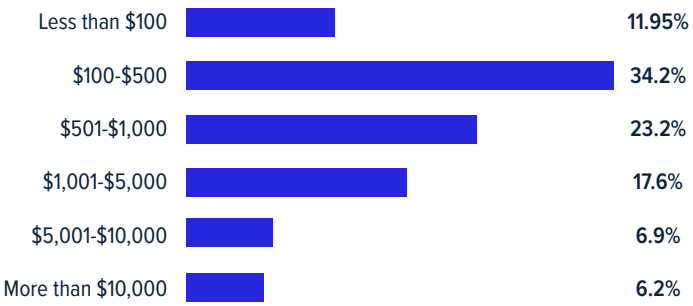
Yes No Not sure

If so, was financial loss incurred?



Yes No

If so, what was the amount of the financial loss incurred?



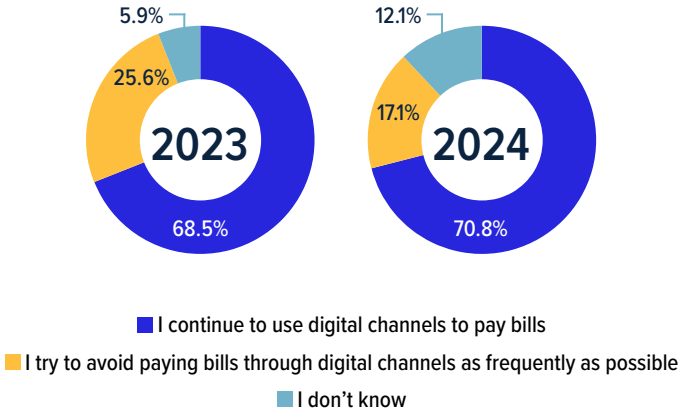
Fraud is impacting trust in data security

Fortunately among the victims of online identity theft, **70%** said they continue to use digital channels to pay bills. Indeed, consumers generally are significantly less likely than in 2023 to say they try to avoid paying bills through digital channels as frequently as possible (**Figure 5**).

These findings demonstrate how entrenched digital bill payment channels have become and are testament to the convenience of the customer experience created by billers and the control they offer to consumers.

Figure 5

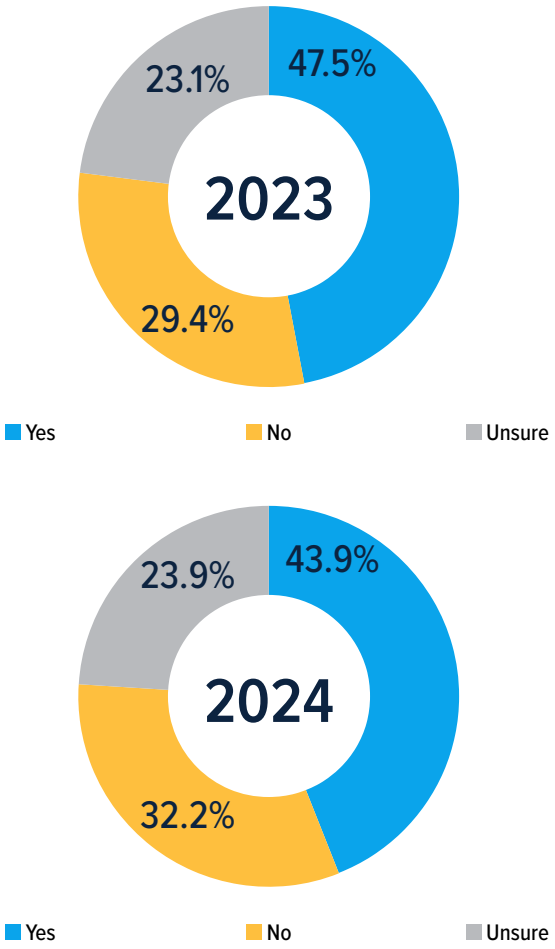
Has this impacted your willingness to pay bills digitally?



The bad news, however, is that trust in data security has taken another hit. Fewer consumers believe their data is more secure than it was five years ago, a belief that has been trending significantly downward for a number of years now (**Figure 6**). As convenient as consumers might find digital channels, and with so many falling victim to identity fraud, these experiences will be shared via word of mouth and even amplified by media coverage in some situations.

Figure 6

Do you believe your data is more secure than it was five years ago?



Consumers need more encouragement from billers on password hygiene

Consumers are most likely to strengthen passwords, create strong passwords, and not reuse passwords when it comes to helping to prevent fraud (**Figure 7**). It's also welcome news to hear that they are significantly more likely than in 2023 to say that two-factor authentication and/or facial recognition would make them feel more secure in utilizing mobile and digital platforms.

Figure 7

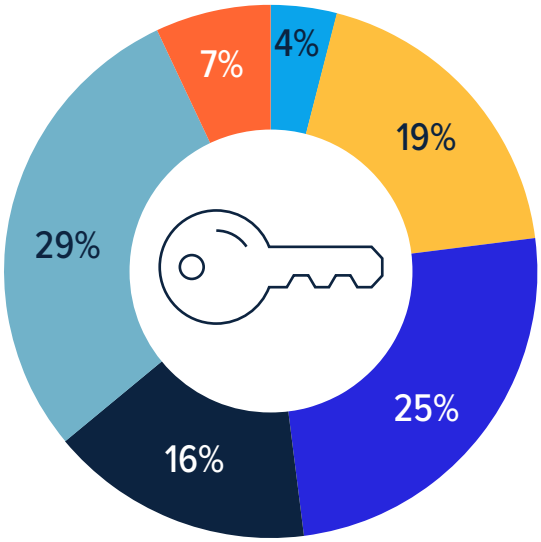
What fraud prevention action have you taken to date?

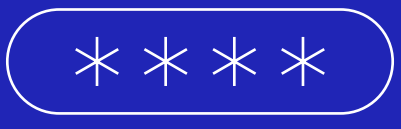
57.8% Strengthened password	**40.9%** Created strong/don't reuse passwords
38.2% Shredded or destroyed statements and mail	**37.9%** Set up multifactor authentication (MFA)
33.8% Restricted what is shared on social media	**26.8%** Eliminated paper statements/mailed payments
25.2% Put restrictions or locks on accounts	**24.3%** Set account alerts with low threshold
20.8% Enlisted credit monitoring services such as IdentityForce, etc.	**17.9%** Opted in for biometrics
14.3% Set up credit lock/monitoring service (Lifelock)	**13.6%** Froze credit with bureaus (directly with 3 credit bureaus)
11.0% Eliminated social media accounts	**2.4%** Other

Of those consumers that report rarely changing passwords, or only doing so when prompted (**Figure 8**), we also see evidence that biller outreach to prompt customers to change their passwords in the interest of increased security is both needed and should be increased. It's on billers to step up here, because apathy around password hygiene, such as regularly updating passwords and not using the same password across multiple biller sites (reported by **14%** of consumers), plays right into the hands of fraudsters.

Figure 8

How often do you change your passwords?





Consumers want to hear from billers on how to protect their data

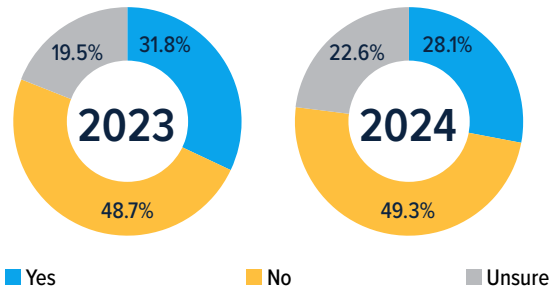
Our survey also reveals an opportunity for billers to attract and retain customers through building a reputation for helping customers with their own data security. Fewer than one in three consumers believe companies properly educate them on how they can keep data secure, which is significantly down compared to 2023 (**Figure 9**).

This is supported by a report from Visa that states, "***Balancing robust security controls while removing friction from transactions and customer interactions is a critical need***."[1]

Billers could respond to these findings by stepping up efforts to educate consumers around risks such as phishing, for example, which is a major on-ramp for online identity theft and account takeovers.

Figure 9

Do you believe companies properly educate consumers on how they keep data secure?



Is consumer fear of scams making debt collection harder for billers?

There are signs from our survey that consumer concerns around security and awareness of scams might be making debt collection harder.

Among consumers who have ever had an overdue bill, 34% say they avoid communications from debt collectors because they're not comfortable sharing financial information with strangers (**Figure 10**).

Customers would instead overwhelmingly prefer to set up their own arrangements for dealing with their arrears, either online or via their mobile.

Figure 10

43% Rather set up arrangements on my own on a website or mobile device

35% Nervous about communicating with debt collectors

34% Not comfortable sharing financial information with strangers

29% Embarrassed to be behind on my payments

27% Unable to make the payments

26% Scared about the consequences

17% Do not understand how the process works

[1] *https://usa.visa.com/visa-everywhere/blog/bdp/2023/07/12/top-5-trends-1689206366692.html*

In summary: Adapt your customer experience for increasingly security-conscious consumers

Rising digital payments adoption provides the backdrop for the continued and troubling impact of online identity theft and related risks such as account takeovers.

And while consumers aren't helping with poor password hygiene, we see that there is also scope for billers to double down on their multidimensional fraud prevention and detection strategies. That means combining new technology to secure their increasingly popular digital channels, such as AI and biometric/multifactor authentication, with educating customers on the steps they can take to reduce the threat of fraud.

They can also swap unsolicited calls from human collection agents, whose authenticity is likely to be questioned by scam-conscious consumers, for virtual interactions such as those provided by ACI® Virtual Collection Agent™. This would enable them to offer past-due consumers a non-confrontational, self-service, and secure platform where they can make payment arrangements on their own time.

Taken together, these changes would help billers better protect their customers and lower costs, while delivering more of the bill pay experiences that consumers expect and prefer.

Further reading: How can organizations use machine learning with their existing fraud management teams?

Machine learning is the perfect supplement to any fraud management strategy, able to automatically identify both complex and subtle fraud patterns that might otherwise be difficult for humans to detect.

By integrating machine learning tools into existing workflows and using them to rapidly analyze large datasets, organizations can free up fraud analysts to investigate more sophisticated cases and refine overall fraud management strategies. This not only increases efficiency, but also empowers analysts to deploy their expertise where it's needed most, optimizing team performance and improving the organization's security posture.

Today's fraudsters are leveraging the latest AI tools to target consumers to steal their identities and compromise their accounts, resulting in more than $10 billion in fraud losses in 2023, according to the Federal Trade Commission.[2] Billers need to remain vigilant and ensure that they are not only aware of new tactics, but also armed with the latest fraud fighting tools to protect their customers and their bottom line.

[2] https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public

Find out more in
From data to defense: The role of machine learning in fraud prevention and
Fraud prevention powered by artificial intelligence

Fraud glossary

Term	Definition
Account takeover (ATO) fraud	Account takeover (ATO) fraud occurs when an unauthorized user gains access to a customer account. Although this could easily occur by sharing login information with another party, the most common culprit for ATO fraud is data breaches. Fraudsters can illegally obtain stolen login credentials and use this information to gain access to a person's private accounts.
Authorized push payment (APP) fraud	When someone is tricked into authorizing a payment to an account controlled by a criminal. Particularly prevalent and difficult to control when the payment is made via instant payments.
Billing fraud	Billing fraud involves intentionally submitting false or inflated invoices for goods or services that were never provided or were overcharged.
Bust-out fraud	When someone applies for credit, establishes a normal spending pattern, and then maxes out the account without intending to pay the balance. This can be done under their own name, or with a stolen or fake identity.
Card cracking	Card cracking fraud is a deceptive practice where cybercriminals trick people into sharing their banking information, such as debit card details and PINs. The goal is to gain access to a person's bank account, which can then be used for illegal activities like identity theft and money laundering.
Card testing	Card testing occurs when fraudsters test card numbers online, including biller websites. They typically validate account details or try different combinations of data to uncover full card details.
Card-not-present (CNP) fraud	A type of credit card fraud that occurs when a criminal uses stolen card information to make a purchase without presenting the physical card to a merchant or biller. CNP fraud can happen online, by phone, or by mail, and is a major concern for companies that accept payments remotely.
Catfishing	A form of social engineering where fraudsters and criminals create fake online identities to lure people into emotional or romantic relationships for personal or financial gain.
Chargeback fraud	When a customer disputes a legitimate transaction.
Clean fraud	When fraudsters use accurate information to impersonate a cardholder and make fraudulent transactions that appear legitimate.
Clickjacking	When a fraudster targets someone to click a link, either to get them to install malware or to try to "phish" them, a related term that involves getting a user to enter personal information via a fake website.
Enumeration attack	Perhaps better known as a brute force attack, an enumeration attack occurs when a hacker attempts repeatedly — using automated scripts or software — to submit card-not-present transactions through a combination of payment values, such as a primary account number (PAN), a card's verification value (CVV2), expiration date, and zip code. When they get an approval, they know they have legitimate payment account details.
Fraud farms/click farms	A large-scale operation that uses groups of low-paid workers to carry out fraudulent attacks. These workers are paid a fee to perform actions such as clicking on ads, registering for accounts, or completing CAPTCHAs. The goal is to artificially boost the status of a product, service, or website for a client.
Merchant identity fraud	Very similar to consumer identity fraud, merchant identity fraud involves criminals setting up a fraudulent merchant account after illegally obtaining a business' identification information. The fraudster will use this newly created "business" to place charges on customers' credit cards, then terminate the account and walk away with the money, leaving the legitimate business to deal with a slew of chargebacks, customer complaints, and fraud reports.
Money muling	A type of money laundering where someone is recruited to move illegally obtained money for another person. Money mules may be unaware that they are helping criminals, or they may be motivated by the promise of easy money.
Online identity theft	Online identity theft involves the unauthorized acquisition and use of personal data. This stolen data can include names, passwords, banking details, or credit card numbers used to commit future payments fraud.
P2P (peer-to-peer) payments fraud	Payments fraud in peer-to-peer payments occurs through card cracking, money muling, and falsifying billing sites or customer service contacts.

Fraud glossary

Term	Definition
Pagejacking	Involves copying a web page from a legitimate site and duplicating it on a fraudulent site. The aim is to divert internet traffic from the genuine site to the counterfeit one, leading to harmful outcomes like stolen payments information, which may be used for future fraud attempts.
Phantom billing	Billing for services or supplies that were never received.
Pharming	The fraudulent practice of directing internet users to a bogus website that mimics the appearance of a legitimate one to obtain personal information such as passwords, account numbers, etc.
Phishing	This type of attack typically involves a fraudster sending an email that informs the recipient that their account has been "compromised" and they need to reset their password. The goal of email phishing is to get the recipient to willingly disclose their private login credentials or any other sensitive information the fraudster might want.
Ransomware	A type of malicious software designed to block access to a computer system until a sum of money is paid.
Skimming	When a criminal uses a device to steal debit or credit card information at the point of sale.
Smishing	This is a type of phishing attack that uses SMS text to target unknowing victims. Smishing tactics are very similar to how an email phishing attack works. Fraudsters send a text informing victims that their account has been compromised and they need to share their login information to gain access to the account. Once the fraudster has the login credentials, they change the password and block the victim from accessing the account.
Social engineering	A manipulation technique that exploits human error to gain private information, access, or valuables.
Spear phishing	The fraudulent practice of sending emails ostensibly from a known or trusted sender to induce targeted individuals to reveal confidential information.
Synthetic identity fraud	Occurs when the perpetrator creates a fictitious identity with false information. They may use stolen Social Security numbers or other personally identifiable information (PII) to create a unique profile that looks like an actual person.
Vishing	Vishing follows the same concept as phishing attacks, but fraudsters use a voice call. A popular vishing attack is the "extended vehicle warranty" scam. Bad actors call a potential victim to inform them that their vehicle's extended warranty is expiring, and they need to disclose their banking credentials to ensure the new warranty is properly set up.

ACI Speedpay Pulse Methodology

The ACI Speedpay Pulse is a longitudinal consumer billing and payment trends research study conducted by Brownstein Group in partnership with ACI Worldwide. Each ACI Speedpay Pulse data set includes responses from a survey of at least 3,000 unique respondents (no repeat participation within a one-year period). Each survey sample is U.S. Census-balanced among adults age 18 and older who are responsible for submitting payments for at least two of their household's monthly bills. Survey margin of error is less than 1.8% for questions answered by the entire sample. Questions with a smaller base will have a higher margin of error. If presented, statistical testing is at the 95% confidence level.

LEARN MORE
www.aciworldwide.com
@ACI_Worldwide
contact@aciworldwide.com

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

PLS2058 08-24