Aite PARTNER. ADVISOR. CATALYST.

Combating False Declines Through Customer Engagement

MAY 2017

Julie Conroy

Sponsored by: iovation®

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

IMPACT POINTS

- In this research effort, sponsored by iovation, Aite Group surveyed 1,095 U.S. consumers in January 2017 to better understand the impact of false declines on the customer experience. Based on quantitative consumer research, the report looks at the likelihood that false declines at the point of sale (POS) will prompt consumers to leave their financial institution (FI). The report also looks at technologies that can reduce false declines as well as consumers' propensity to proactively engage with these technologies.
- The problem is significant; in the U.S. market alone, US$264 billion in card transactions were falsely declined due to suspicion of fraud in 2016.
- Millennials are far less forgiving of false declines than are older generations. Of the millennial cohort, 59% say that they would be very or somewhat likely to leave their FI due to a credit card false decline; in contrast, just 21% of seniors would be inclined to leave their issuer.
- Higher-income consumers display a greater propensity to leave their FI in the event of a false decline than do low-income cardholders. Forty-four percent of consumers with income over US$100,000 per year and 48% of consumers with income between US$75,000 and US$99,999 per year say they are very likely or somewhat likely to leave their FI due to a mistakenly declined credit card transaction.
- The majority of consumers across all age groups are open to an additional prompt for identity verification if there is suspicion of fraud. Sixty-five percent of seniors and boomers say it's fine for their issuer to request proof of identity if there is suspicion of fraud; 59% of Gen Xers and 54% of millennials agree.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

INTRODUCTION

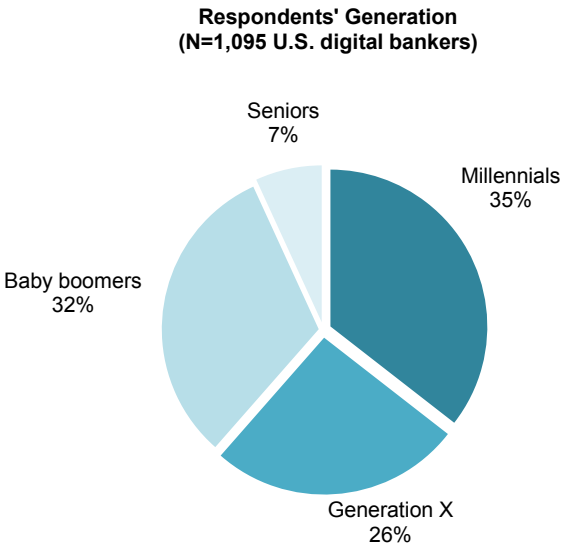
Most cardholders have experienced it—that feeling of embarrassment and frustration at the POS when a payment card is mistakenly declined due to suspicion of fraud. False declines, which occur when a good transaction by the authorized cardholder is erroneously declined, happen far more often than issuers and merchants would like. False declines not only result in lost revenue opportunities but also create unhappy customers, which is bad business for both the merchant and the card-issuing bank.

This Impact Report examines the impact of false declines on consumers' relationships with their FI. Based on quantitative consumer research, it looks at the likelihood that false declines at the POS will prompt consumers to leave their FI. The report also looks at technologies that can reduce false declines as well as consumers' propensity to proactively engage with these technologies.

METHODOLOGY

In this January 2017 research effort, sponsored by iovation, Aite Group surveyed 1,095 U.S. consumers to better understand the impact of false declines on the customer experience. The sample is in proportion to the U.S. population for age, gender, income, geographic region, and race. The data has a margin of error of three points at the 95% level of confidence. Seniors are defined as individuals who were born in or before 1946, baby boomers between 1946 and 1964, Gen Xers between 1965 and 1980, and Gen Yers or millennials between 1981 and 2000 (Figure 1 and Figure 2).

Figure 1: Survey Respondents by Generation

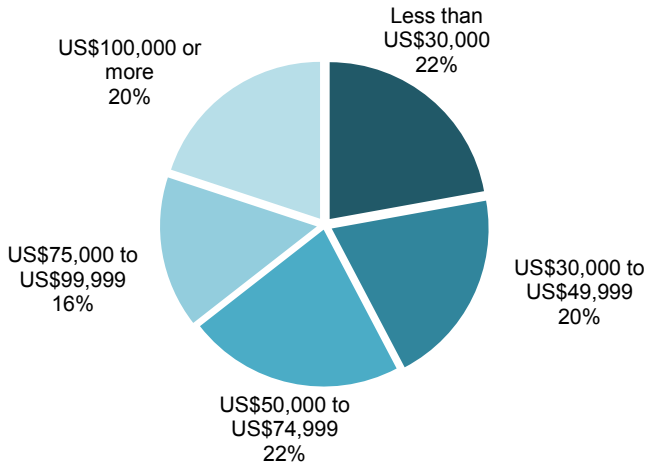


Source: Aite Group survey of 1,095 U.S. consumers, January 2017

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 2: Survey Respondents by Income

Q. Including employment, the government, and other sources of income, what was your 2016 household income? (N=1,095 U.S. digital bankers)



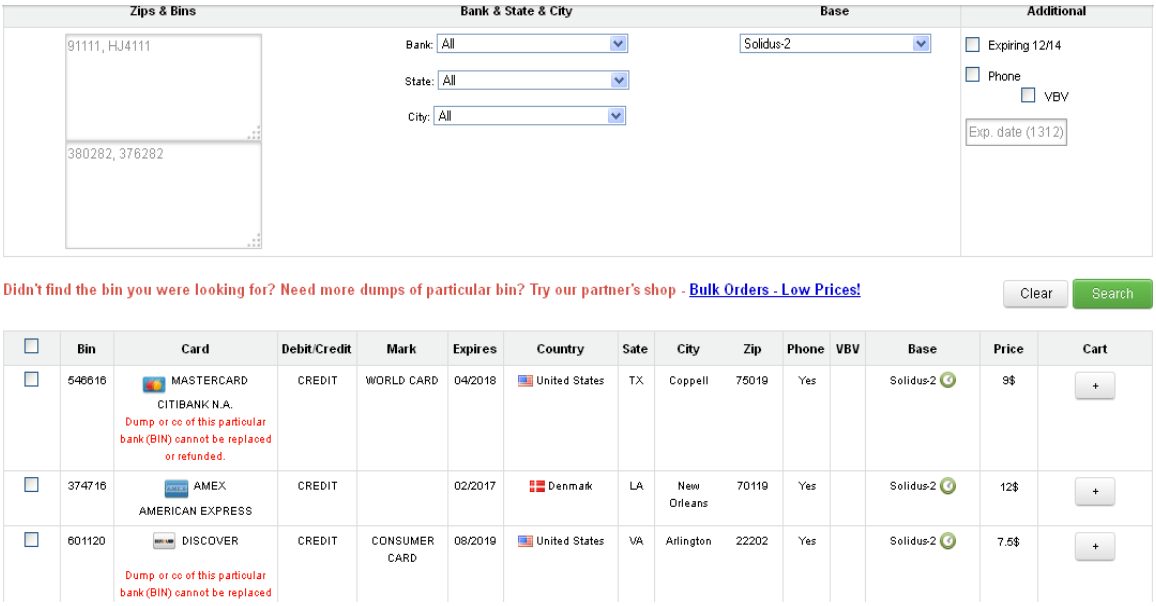
Source: Aite Group survey of 1,095 U.S. consumers, January 2017

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

THE MARKET DRIVERS

Large-scale card compromises, particularly via POS malware, have become distressingly commonplace over the past few years. As a result, organized crime rings not only have ample sources of stolen card data but often also possess the zip code in which the genuine card was originally used, as illustrated in the underground card sales site shown in Figure 3. This key data element enables the rings to perpetrate their card fraud in the same geographic footprint as the genuine cardholder, making it much more difficult for card issuers' analytical models to identify fraudulent transactions.

Figure 3: Compromised Cards for Sale on the Underweb



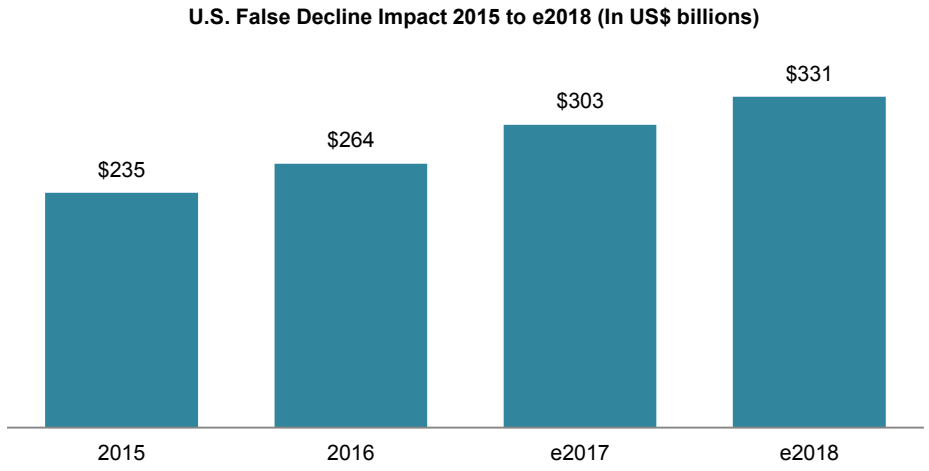
Source: Krebsonsecurity.com

As a result, issuers relying on traditional analytical models are left with a no-win situation. Either they can be more draconian with their authorization strategies, which stops more fraud but also results in more false declines, or they can absorb more fraud losses. The problem is significant; in the U.S. market alone, US$264 billion in card transactions were falsely declined due to suspicion of fraud in 2016 (Figure 4).[1] This estimate does not include transactions declined due to lack of available credit line (for credit card) or insufficient balance (for debit card). Card-not-present (CNP) transactions have a much higher likelihood of being declined due to the higher inherent risk. The average decline rate for a CNP transaction is 15% to 20%, versus 2% to 3% for card-present transactions.

1. See Aite Group's report *Chargebacks and False Declines: Cards' Ugly Underbelly*, August 2016.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 4: U.S. False Decline Problem



Source: Aite Group

Table A describes the key market trends and implications surrounding false declines today.

Table A: Market Trends and Implications

Market trends	Market implications
Increasing volume and sophistication of data breaches	While businesses protecting their sensitive data have to be perfect 100% of the time in their efforts to safeguard sensitive data, criminals just need to be successful once in their myriad attempts to make off with a treasure trove of data. The organized crime rings behind the bulk of the attacks are persistent, nimble, technically savvy, and sophisticated.
Effective fraud mitigation is now a competitive differentiator	The concept that "fraud is not a competitive issue" is no longer an absolute truism. Fraud executives are increasingly held accountable for the customer experience as well as fraud losses. As a result, many FIs are prioritizing solutions that can both stem losses and help provide a seamless customer experience.
The mobile device presents new opportunities to engage the consumer in improving the customer experience	The now-ubiquitous smartphone can enable a variety of signals and authenticators that issuers can leverage to engage their customer in the effort to better inform authorization decisions.

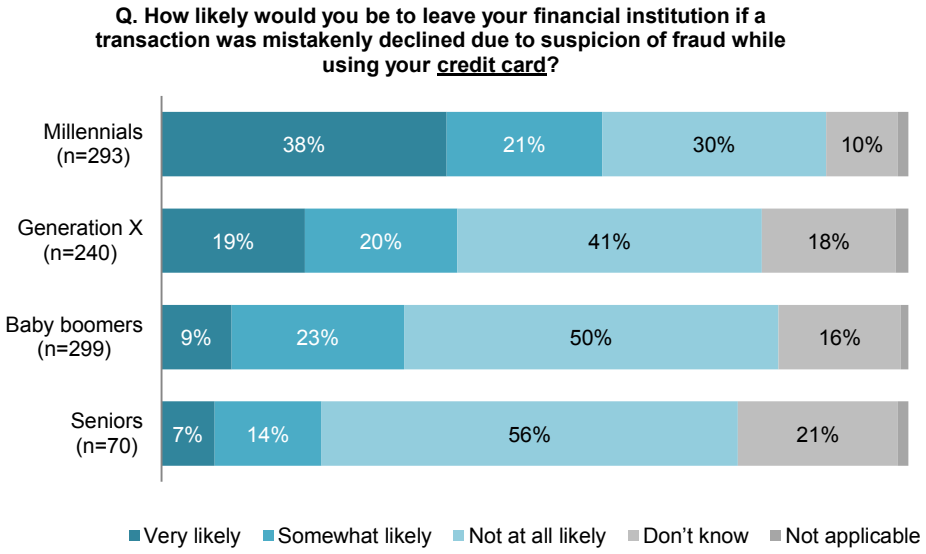
Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

FALSE DECLINES: THE CUSTOMER-EXPERIENCE KILLER

False declines have a material impact on an issuer's business. While lost transaction revenue is certainly painful, this is actually the least of an issuer's worries. The damage to the issuer's relationship with its customer is of far greater concern. The impact varies widely by generation, as shown in Figure 5. Millennials are far less forgiving than are older generations. Of the millennial cohort, 59% say that they would be very or somewhat likely to leave their FI due to a credit card false decline; in contrast, just 21% of seniors would be inclined to leave their issuer.

Figure 5: Consumers' Attitudes Toward Credit Card False Declines

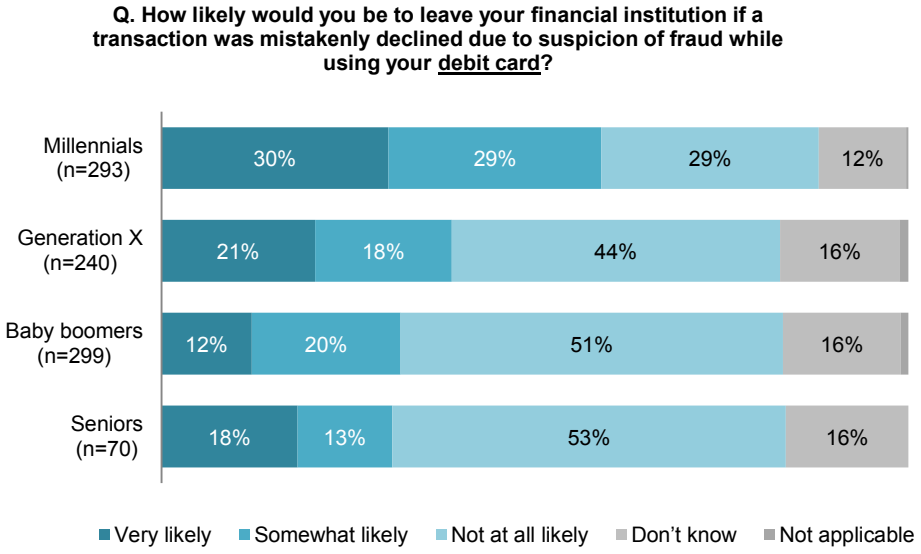


Source: Aite Group survey of 1,095 U.S. consumers, January 2017

Fifty-nine percent of millennials would be likely to leave their FI due to a debit card false decline, followed by 39% of Gen Xers, 32% of baby boomers, and 31% of seniors (Figure 6).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

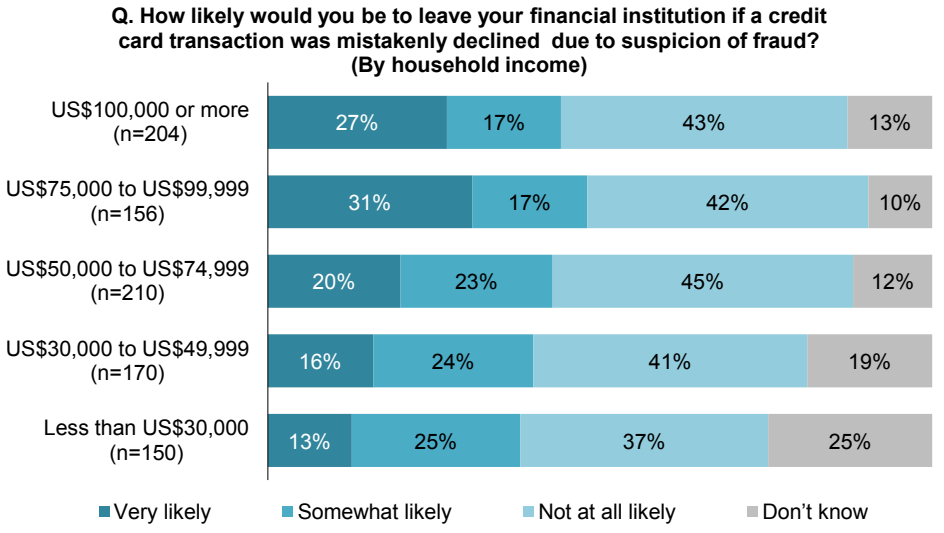
Figure 6: Consumers' Attitudes Toward Debit Card False Declines



Source: Aite Group survey of 1,095 U.S. consumers, January 2017

Higher-income consumers display a greater propensity to leave their FI in the event of a false decline. Forty-four percent of consumers with income over US$100,000 per year and 48% of consumers with income between US$75,000 and US$99,999 per year say they are very or somewhat likely to leave their FI due to a mistakenly declined credit card transaction. These consumers are often among FIs' most profitable customers, so their relatively low tolerance for false declines should factor prominently into FIs' authorization decisions (Figure 7).

Figure 7: Consumers' Attitudes Toward False Declines by Income

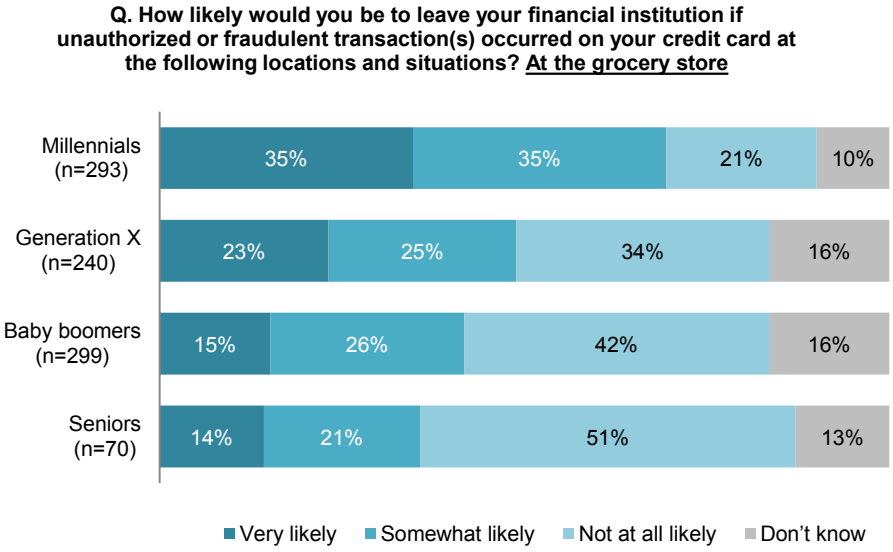


Source: Aite Group survey of 1,095 U.S. consumers, January 2017

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

The context of the transaction also factors into consumers' tolerance for fraud, although the trend toward millennials exhibiting less tolerance than older generations continues to hold true (Figure 8).

Figure 8: Propensity to Leave FI Due to Unauthorized Transactions at the Grocery Store

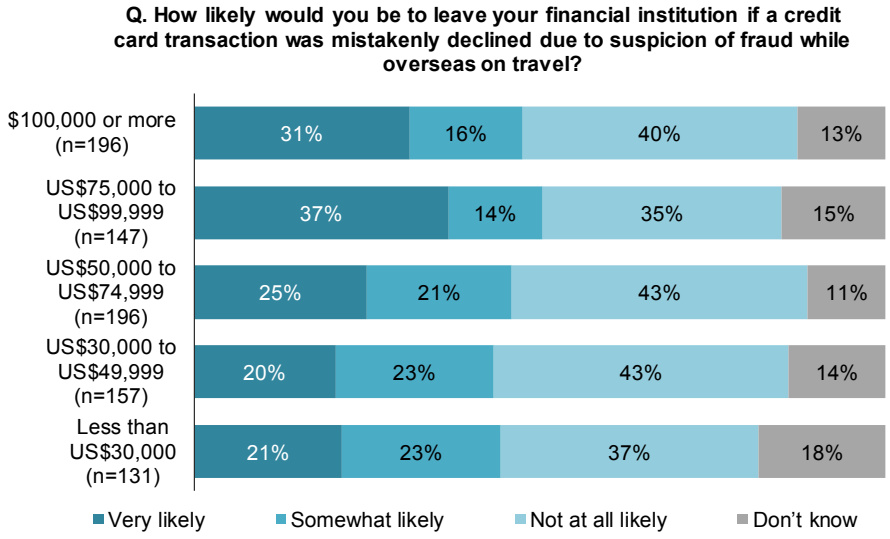


Source: Aite Group survey of 1,095 U.S. consumers, January 2017

The impact of false declines during overseas travel adversely impacts FIs' relationships with their higher-income consumers more so than with lower-income consumers. Forty-seven percent of consumers with incomes greater than US$100,000 and 51% of consumers with incomes between US$75,000 and US$99,999 would be inclined to leave their FI if their credit card is mistakenly declined while traveling overseas (Figure 9). This makes sense—higher-income consumers are more likely to travel internationally, and the hassle and inconvenience of a false decline is often greatly exacerbated for international travelers.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 9: Impact of False Declines on Overseas Travelers



Source: Aite Group survey of 1,095 U.S. consumers, January 2017

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ENGAGING THE CUSTOMER IN THE AUTHORIZATION DECISION

Issuers have a number of options available to them as they seek to address the problem of false declines. Improving their analytics capabilities is one avenue. The confluence of low data storage costs and rapidly increasing processing speeds has enabled advanced analytics techniques to significantly improve upon legacy models.[2]

Analytics can't do it all, however. Thanks to the increasing ubiquity of the smartphone, a range of powerful authentication capabilities are now available. These can be used either to feed additional data inputs into analytic routines, or to create a dialogue between the FI and the customer to help inform the transaction decision (Table B).

Table B: Authentication Methods

Authentication type	Description
Mobile geolocation	This technology uses sensors native to the mobile device to identify its location.
Device fingerprint (or device identification)	Device identification technology examines a combination of identifiable hardware and software attributes associated with a computer or mobile device.
Facial recognition	Facial recognition uses the device's video recorder to capture the end user's face and typically requires the user to blink to perform liveliness check.
Fingerprint biometric	The fingerprint biometric leverages a device's embedded fingerprint reader; remote-channel use cases are currently focused on the mobile channel.
Voice recognition	Voice recognition creates a unique biometric driven by the characteristics of the end user's voice.
One-time password (OTP)	An OTP is sent via SMS message to the cardholder.
Two-way text	An SMS message is sent to the consumer, to which they can reply, either approving or denying the transaction.
Mobile app push	A message is pushed to the consumer from the issuer's mobile app, to which they can reply, either approving or denying the transaction.

Source: Aite Group

Incorporating these factors into the authorization decision can take place in a number of different ways, as described in Table C. Chip-card transactions and mobile payment transactions that use the phone's secure element are inherently safer due to the dynamic data generated by the chip. In theory, these transactions should have fewer false declines than mag stripe and CNP transactions.[3]

2. See Aite Group's report *Machine Learning for Fraud Detection: The Substance Behind the Buzz*, April 2017.

3. See Aite Group's report *EMV: Issuance Trajectory and Impact on Account Takeover and CNP*, May 2016.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Table C: Combining Authentication With the Authorization Decision

Transaction type	Authenticator(s)	Use case
Card at POS	Mobile geolocation	If the consumer has the issuer's mobile app on their device, the geolocation can be captured. If the mobile device is in close proximity to the transaction location, that intelligence can be used to reduce the possibility of false decline.
	Two-way text Mobile app push	After a suspicious transaction, the issuer pushes a message to the cardholder via two-way text or mobile app push, asking if the transaction was genuine.
Mobile payment at POS using secure element	Mobile geolocation	If the consumer has the issuer's mobile app on their device, the geolocation can be captured. If the mobile device is in close proximity to the transaction location, that intelligence can be used to reduce the possibility of false decline.
	Device fingerprint Facial recognition Fingerprint biometric Voice recognition	These authenticators can be captured prior to the transaction, and a message will be transmitted with the authorization message that the transaction is authenticated, which should significantly reduce the possibility of a false decline. While device fingerprint is transparent to the end user, the use of biometrics will require cardholder education.
	Two-way text Mobile app push	After a suspicious transaction, the issuer pushes a message to the cardholder via two-way text or mobile app push, asking if the transaction was genuine.
Mobile payment at POS using cloud-based wallet	Mobile geolocation	If the consumer has the issuer's mobile app on their device, the geolocation can be captured. If the mobile device is in close proximity to the transaction location, that intelligence can be used to reduce the possibility of false decline.
	Two-way text Mobile app push	After a suspicious transaction, the issuer pushes a message to the cardholder via two-way text or mobile app push, asking if the transaction was genuine.
CNP	Mobile geolocation	If the consumer has the issuer's mobile app on their device, the geolocation can be captured. If the mobile device is in close proximity to the transaction location, that intelligence can be used to reduce the possibility of false decline.
	Device fingerprint	If the 3-D Secure protocol is invoked, the device fingerprint is captured and figures into the issuer's risk-based authentication decision.[4]

4. See Aite Group's report *Not Your Father's 3-D Secure: Addressing the Rising Tide of CNP Fraud*, February 2016.

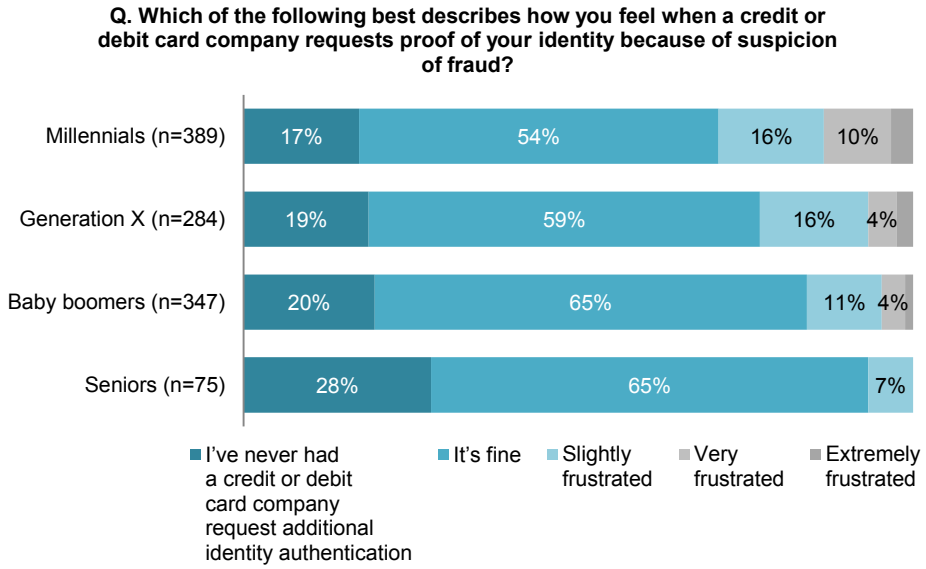
101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Transaction type	Authenticator(s)	Use case
	Facial recognition Fingerprint biometric Voice recognition	In 3-D Secure transactions, the issuer chooses the form of stepped-up authentication. One-time password is the current prevailing method, although many issuers are contemplating other forms due to the susceptibility of the OTP to SIM swaps and other workarounds.
	Two-way text Mobile app push	After a suspicious transaction, the issuer pushes a message to the cardholder via two-way text or mobile app push, asking if the transaction was genuine.

Source: Aite Group

When it comes to transactional security, however, consumers have shown that the process does not always have to be completely transparent. The majority of consumers across all age groups are open to an additional prompt for identity verification if there is suspicion of fraud (Figure 10). Sixty-five percent of seniors and boomers say it's fine for their issuer to request proof of identity if there is suspicion of fraud; 59% of Gen Xers and 54% of millennials agree. The decreasing level of acceptance across generations is likely the result of younger generations having a higher proportion of digital natives with high expectations for seamless customer experiences.

Figure 10: Consumers' Attitudes Toward Identity Verification by Age Group

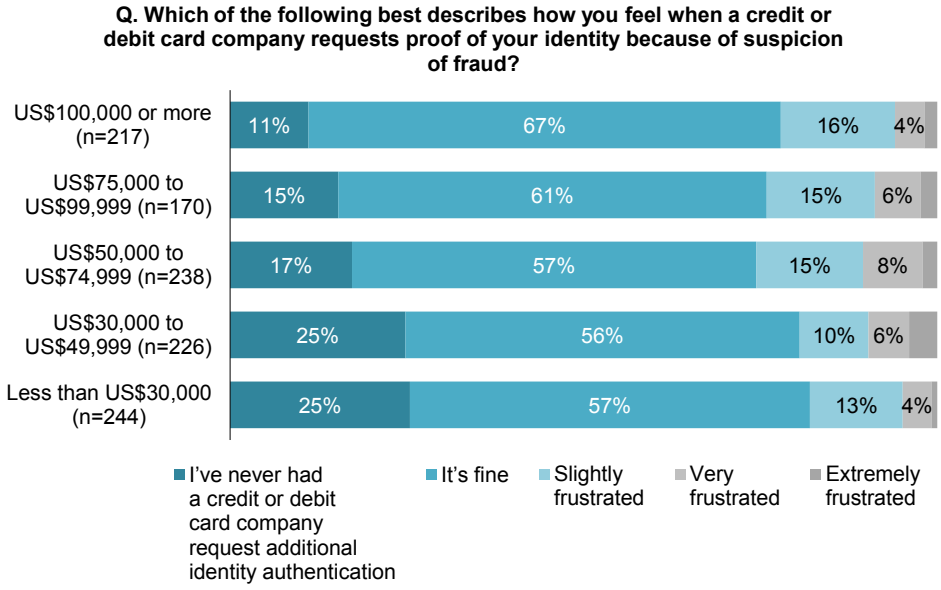


Source: Aite Group survey of 1,095 U.S. consumers, January 2017

As shown in Figure 11, the majority of consumers in all income groups are also open to requests for additional proof of identity. Higher-income individuals are the most receptive, with 67% of individuals whose income is above US$100,000 stating that they are fine with additional identity verification requests.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 11: Consumers' Attitudes Toward Identity Verification Requests by Income

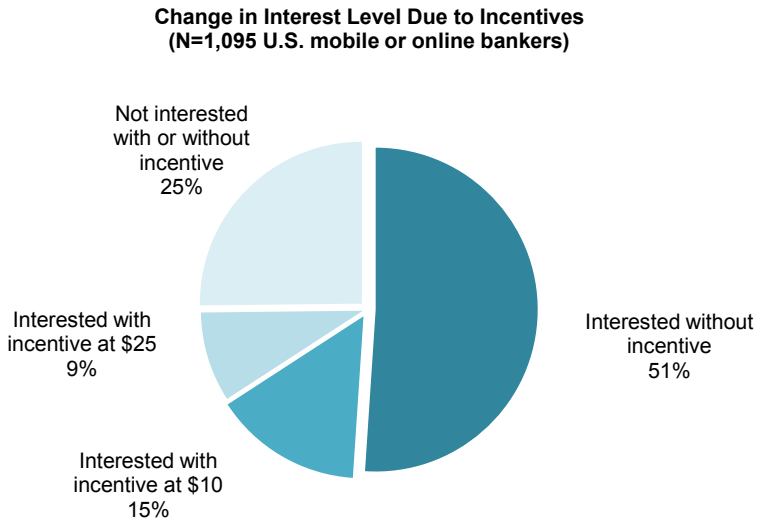


Source: Aite Group survey of 1,095 U.S. consumers, January 2017

This openness to engagement represents new opportunities to FIs to reduce false declines. The path forward is not an easy one—changing customer behavior never is. Well-constructed education campaigns about the benefits of the various forms of mobile authentication, however, and the ways in which it can help reduce false declines can help begin the habituation process. Monetary incentives can also potentially help speed consumer adoption. When asked whether a monetary incentive of US$10 or US$25 would encourage consumers to proactively adopt a range of authentication mechanisms (e.g., two-way text, voice recognition, mobile app push, or voice recognition), 51% of consumers indicate that they'd be willing to engage without an incentive, while another 24% of consumers are motivated to engage by the monetary incentive (Figure 12).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 12: Impact of Incentives on Consumer Engagement



Source: Aite Group survey of 1,095 U.S. consumers, January 2017

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

CONCLUSION

False declines are potential relationship killers and occur far too often. Here are a few recommendations for issuers as they work to minimize them:

- **Invest in advanced analytics.** Analytics have made great strides over the past decade and are particularly useful when fueled with data about the customer and the transaction itself.
- **Expand your options for customer engagement.** The ubiquitous presence of the mobile device provides a variety of new ways to harvest contextual and/or authenticating data.
- **Know your customer.** Based on their age group and income level, customers will react to false declines in different ways. Incorporate this knowledge into your customer engagement strategies.
- **Educate, educate, educate.** Whether they like it or not, customers have a key role to play in helping to minimize both fraud and false declines. Most are unaware of ways in which they can participate, however. It is incumbent on institutions to not only educate consumers but also tailor their messaging by generation for maximum efficacy.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

RELATED AITE GROUP RESEARCH

Machine Learning for Fraud Detection: The Substance Behind the Buzz, April 2017.

Moving Beyond the Password: Consumers' Views on Authentication, March 2017.

Global Consumer Survey: Consumer Trust and Security Perceptions, February 2017.

Global Security Engagement Scorecard™, November 2016.

Chargebacks and False Declines: Cards' Ugly Underbelly, August 2016.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

AUTHOR INFORMATION

Julie Conroy
+1.617.398.5045
jconroy@aitegroup.com

Research Design & Data:

Sarah Fitzsimmons
+1.617.398.5039
sfitzsimmons@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com