

Global Consumer Survey: Consumer Trust and Security Perceptions

FEBRUARY 2017

Shirley Inscoe



TABLE OF CONTENTS

IMPACT POINTS	4
INTRODUCTION	5
METHODOLOGY	5
THE CONTINUING RISE OF THE MOBILE CHANNEL.....	7
MOBILE WALLET SECURITY	10
RETAILERS	14
IN-PERSON SHOPPING	14
ONLINE SHOPPING	17
FRAUD AND DATA BREACHES	20
STORED DATA	23
PROTECTING CARD AND ACCOUNT INFORMATION	27
CONSUMER FRAUD CONCERNS.....	30
FRAUD EDUCATION	35
CONSUMER RESPONSE TO FRAUD ALERTS.....	39
CONCLUSION	46
RELATED AITE GROUP RESEARCH	47
ABOUT AITE GROUP.....	48
AUTHOR INFORMATION	48
CONTACT.....	48

LIST OF FIGURES

FIGURE 1: COUNTRIES SURVEYED IN 2014 AND 2016	6
FIGURE 2: MOBILE WALLET ADOPTION IN THE AMERICAS	7
FIGURE 3: MOBILE WALLET ADOPTION IN EUROZONE	8
FIGURE 4: MOBILE WALLET ADOPTION IN EMEA (NON-EUROZONE).....	8
FIGURE 5: MOBILE WALLET ADOPTION IN THE ASIA-PACIFIC	9
FIGURE 6: PERCEPTIONS OF MOBILE WALLET DATA SECURITY IN THE AMERICAS	10
FIGURE 7: PERCEPTIONS OF MOBILE WALLET DATA SECURITY IN EUROZONE	11
FIGURE 8: PERCEPTIONS OF MOBILE WALLET DATA SECURITY IN EMEA (NON-EUROZONE)	12
FIGURE 9: PERCEPTIONS OF MOBILE WALLET DATA SECURITY IN THE ASIA-PACIFIC	13
FIGURE 10: IN-PERSON SHOPPING IN THE AMERICAS.....	14
FIGURE 11: IN-PERSON SHOPPING IN EUROZONE.....	15
FIGURE 12: IN-PERSON SHOPPING IN EMEA (NON-EUROZONE).....	16
FIGURE 13: IN-PERSON SHOPPING IN THE ASIA-PACIFIC.....	17
FIGURE 14: ONLINE MERCHANT SECURITY IN THE AMERICAS	18
FIGURE 15: ONLINE MERCHANT SECURITY IN EUROZONE	19
FIGURE 16: ONLINE MERCHANT SECURITY IN EMEA (NON-EUROZONE)	19
FIGURE 17: ONLINE MERCHANT SECURITY IN THE ASIA-PACIFIC	20

FIGURE 18: STOP SHOPPING IN THE AMERICAS	20
FIGURE 19: STOP SHOPPING IN EMEA.....	21
FIGURE 20: STOP SHOPPING IN THE ASIA-PACIFIC	22
FIGURE 21: SECURITY OF STORED DATA IN THE AMERICAS	23
FIGURE 22: SECURITY OF STORED DATA IN EUROZONE	24
FIGURE 23: SECURITY OF STORED DATA IN EMEA (NON-EUROZONE)	25
FIGURE 24: SECURITY OF STORED DATA IN THE ASIA-PACIFIC	26
FIGURE 25: BEST DATA PROTECTORS IN THE AMERICAS.....	27
FIGURE 26: BEST DATA PROTECTORS IN EUROZONE.....	28
FIGURE 27: BEST DATA PROTECTORS IN EMEA (NON-EUROZONE).....	28
FIGURE 28: BEST DATA PROTECTORS IN THE ASIA-PACIFIC.....	29
FIGURE 29: GREATEST FRAUD RISKS IN THE AMERICAS	31
FIGURE 30: GREATEST FRAUD RISKS IN EUROZONE	32
FIGURE 31: GREATEST FRAUD RISKS IN EMEA (NON-EUROZONE)	33
FIGURE 32: GREATEST FRAUD RISKS IN THE ASIA-PACIFIC	34
FIGURE 33: FRAUD EDUCATION IN THE AMERICAS.....	35
FIGURE 34: FRAUD EDUCATION IN EUROZONE.....	36
FIGURE 35: FRAUD EDUCATION IN EMEA (NON-EUROZONE)	37
FIGURE 36: FRAUD EDUCATION IN THE ASIA-PACIFIC.....	38
FIGURE 37: ACTIONS FOLLOWING SUSPICIOUS ACTIVITY IN THE AMERICAS.....	39
FIGURE 38: ACTIONS FOLLOWING SUSPICIOUS ACTIVITY IN EUROZONE.....	40
FIGURE 39: ACTIONS FOLLOWING SUSPICIOUS ACTIVITY IN EMEA (NON-EUROZONE).....	40
FIGURE 40: ACTIONS FOLLOWING SUSPICIOUS ACTIVITY IN THE ASIA-PACIFIC.....	41
FIGURE 41: CONTACT PREFERENCES IN THE AMERICAS.....	42
FIGURE 42: CONTACT PREFERENCES IN EUROZONE.....	43
FIGURE 43: CONTACT PREFERENCES IN EMEA (NON-EUROZONE).....	44
FIGURE 44: CONTACT PREFERENCES IN THE ASIA-PACIFIC.....	45

IMPACT POINTS

- This Impact Report, based on a Q2 2016 ACI Worldwide-sponsored study of 6,035 consumers in 20 countries, provides an overview of respondent attitudes toward fraud and data protection, and the ways respondents want to engage with firms to minimize fraud. Where applicable, it also compares these results with those from a similar survey in 2014.¹
- Sixty-five percent of consumers indicate they would stop shopping with a given merchant after experiencing fraud or a data breach.
- Even though data breaches have been common, consumer confidence in merchants' ability to protect personal information increased to 43% in 2016 from 34% in 2014, among the 17 countries surveyed in both studies.
- Across all regions, the number one fraud concern is theft by computer hacking.
- In some markets with very strict data security guidelines, such as Germany and Singapore, consumers report some of the lowest levels of confidence in data security and control.
- Mobile wallet and payments adoption tends to be strongest in regions where infrastructure for other electronic payments options, particularly card payments, is less mature.
- Consumers are generally not confident in firms' ability to protect their stored data. Only in the U.S., India, and Thailand do consumers report at least 50% confidence that their stored data is well-protected.
- Consumers are generally willing to interact with organizations to mitigate fraud, and mobile is the primary channel, either voice or electronic, through which they wish to engage. Indeed, 75% of consumers are very interested in receiving a call or SMS message to their mobile device.

1. See Aite Group's report *Global Consumers: Concerned and Willing to Engage in the Battle Against Fraud*, July 2014.

INTRODUCTION

Consumers continue to face a range of changes in technology and in the way technology is applied to financial services. These changes have impacted how people shop, how people pay, and how people perceive the value of their personal data and firms' custodianship of that data. Consumers are more aware of fraud and are concerned about data breaches, with at least 2,260 confirmed data breaches in 2015 alone.²

Importantly, consumers show a willingness to help to combat fraud, particularly by leveraging mobile technology. This willingness opens opportunities for firms to optimize the ways in which they reach out to and communicate with consumers, ultimately improving customer experience while reducing operational costs and fraud losses.

This Impact Report is the second in a two-part series on how financial fraud affects consumers' perceptions.³ The report covers consumer perceptions in 20 different countries in the Americas (North America and South America), Europe, the Middle East, and Africa (EMEA), and the Asia-Pacific region.

METHODOLOGY

ACI Worldwide, a global leader in electronic payments for financial institutions, retailers, and processors, conducted online quantitative market research in April 2016 and surveyed 6,035 consumers. The study was conducted in a total of 20 countries in the following regions:

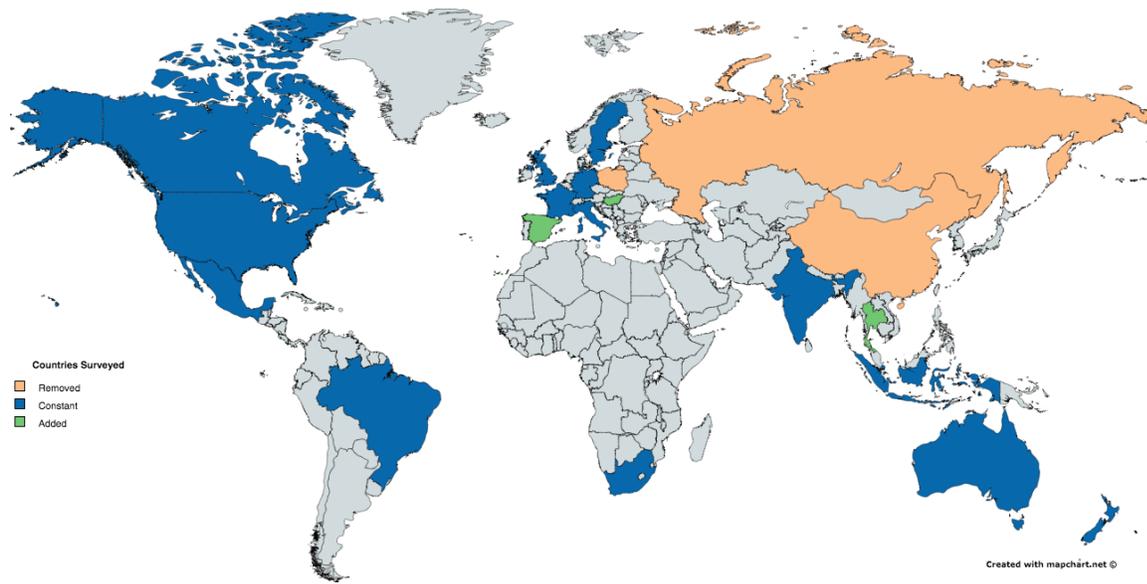
- **The Americas:** Brazil, Canada, Mexico, and the United States
- **EMEA:** France, Germany, Italy, the Netherlands, South Africa, Sweden, the United Arab Emirates (UAE), and the United Kingdom
- **The Asia-Pacific region:** Australia, India, Indonesia, New Zealand, and Singapore

China, Russia, and Poland were removed compared to the 2014 study, and Spain, Thailand, and Hungary were added for 2016.

Figure 1 highlights the countries included in the survey.

2. "2016 Data Breach Investigations Report," Verizon, accessed May 22, 2016, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.

3. See Aite Group's report *2016 Global Consumer Card Fraud: Where Card Fraud Is Coming From*, July 2016.

Figure 1: Countries Surveyed in 2014 and 2016

Source: Aite Group

In total, 6,035 consumers were included in the research—approximately 300 consumers, divided equally between men and women, participated in each of the 20 countries. Of the total, 5,861 own one or more type of payment card—credit card, debit card, or prepaid card. This is the fourth time that ACI has fielded this type of survey, and some comparative results are included from 2012 and 2014.

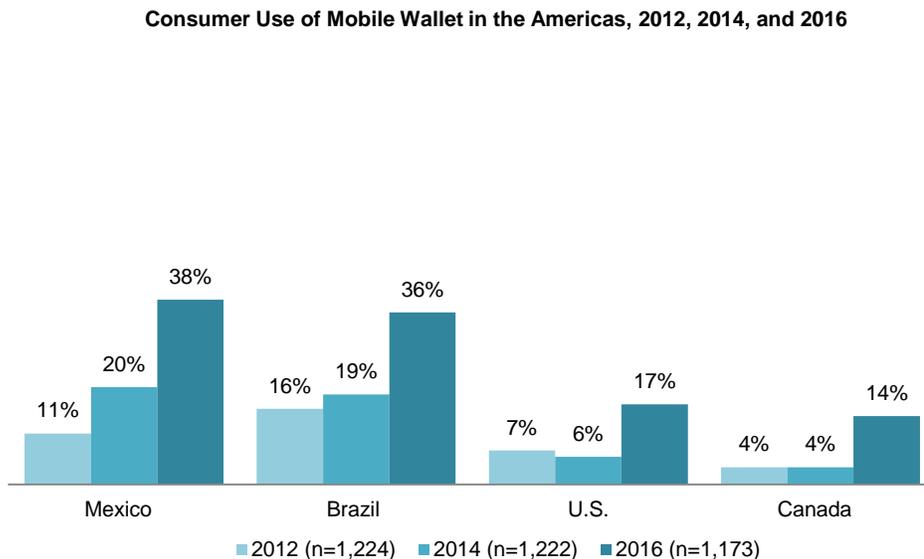
In each country, the data have a margin of error of approximately five points. Statistical tests of significance, where shown, were conducted at the 95% level of confidence.

THE CONTINUING RISE OF THE MOBILE CHANNEL

Mobile banking and payments have been hot topics for a few years, with many predicting the end of traditional card payments and overstuffed “Costanza” wallets. Rumors of cards’ demise have been a bit overblown, particularly in countries with very well-established card payments infrastructure. There is much more adoption of mobile banking and payments in traditionally cash-focused economies.

Mexico and Brazil have much higher rates of mobile wallet adoption than do the U.S. or Canada. Existing infrastructure and entrenched consumer behaviors leave mobile wallets a solution in search of a problem in mature card markets, such as the U.S. and Canada. That said, there is new growth in U.S. and Canada, most likely driven by a combination of more point-of-sale terminals accepting contactless mobile payments and mobile wallets built into many of the newer mobile phones on the market (Figure 2).

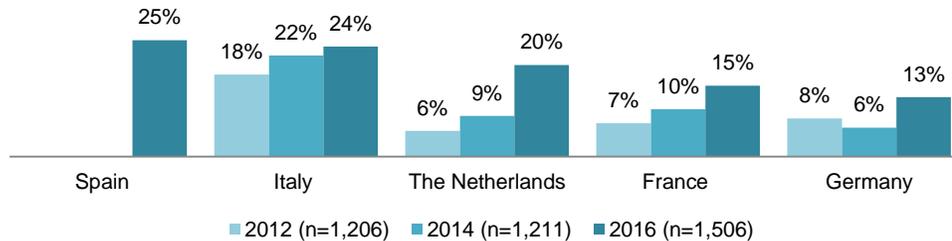
Figure 2: Mobile Wallet Adoption in the Americas



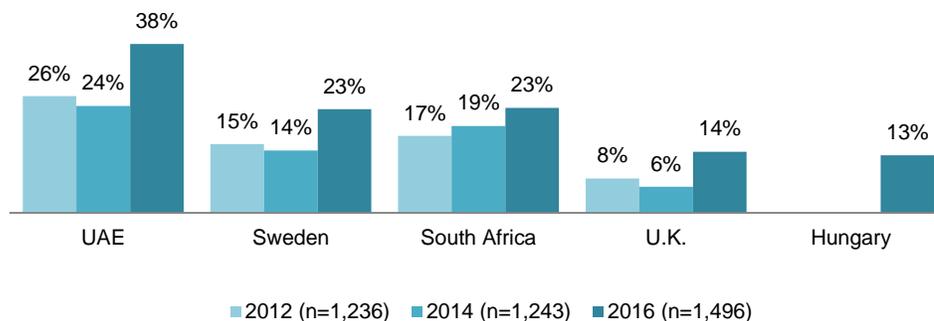
Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016 and Q1 2014, and in 17 countries, Q3 2012

There is a similar pattern across EMEA, where most countries have well-established card payments systems, including contactless e-purse payments for small purchases and transit payments. In fact, some countries in the Nordics are working to eliminate cash. For example, the Danish government has proposed moving toward electronic money for most transactions (Figure 3 and Figure 4).⁴

4. Virginia Harrison, “This Could Be the First Country to go Cashless,” CNN Money, published June 2, 2015, accessed October 10, 2016, <http://money.cnn.com/2015/06/02/technology/cashless-society-denmark/>.

Figure 3: Mobile Wallet Adoption in Eurozone**Consumer Use of Mobile Wallet in EMEA, 2012, 2014, and 2016**

Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016 and Q1 2014, and in 17 countries, Q3 2012

Figure 4: Mobile Wallet Adoption in EMEA (Non-Eurozone)**Consumer Use of Mobile Wallet in EMEA, 2012, 2014, and 2016**

Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016 and Q1 2014, and in 17 countries, Q3 2012

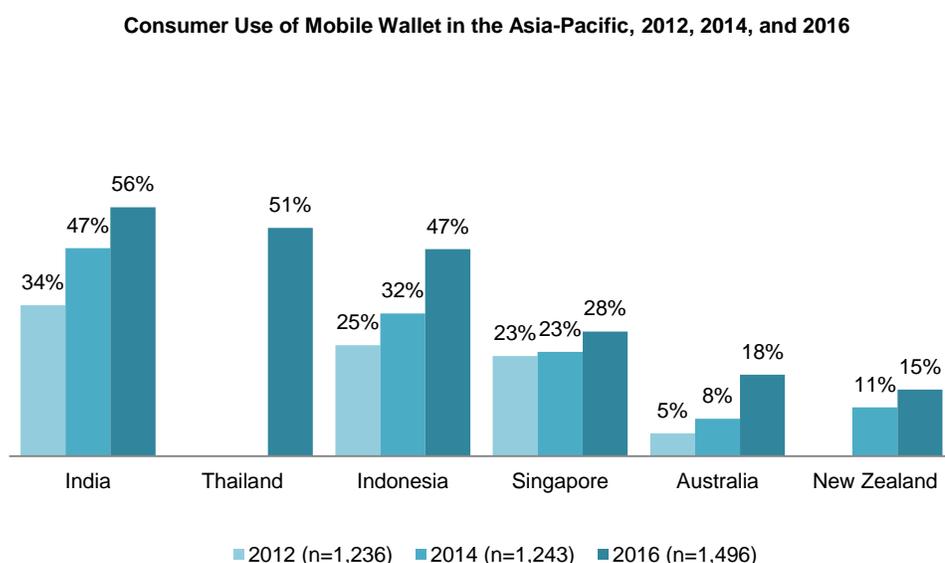
In most cases, mobile wallet adoption in EMEA is generally not showing dramatic increases, and for the most part, adoption is less than 25%. A notable exception is the UAE—part of this higher

adoption rate could hinge on government and industry initiatives supporting contactless, cashless payments in the UAE.⁵

The case in the Asia-Pacific is quite different, with high rates of mobile wallet adoption in India, Thailand, and Indonesia. This is likely due to a large number of mobile-based peer-to-peer payments, and because mobile devices act as the primary access to the internet for many individuals and households. In many cases, individuals may carry multiple devices and thus have multiple wallets.

As with the U.S. and Western Europe, Singapore, Australia, and New Zealand have lower rates of adoption, primarily due to more mature card payments infrastructure and consumers' general comfort utilizing plastic cards (Figure 5).

Figure 5: Mobile Wallet Adoption in the Asia-Pacific



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016 and Q1 2014, and in 17 countries, Q3 2012

Mobile wallet adoption in Asia is generally much higher than in other parts of the world, especially in fast-growing economies such as India, Thailand, and Indonesia. These regions are generally leap-frogging traditional card infrastructure and usage patterns while adopting the latest and greatest technologies. These markets are also very mobile-oriented in that most people's internet connection is through a mobile device rather than a desktop or laptop.

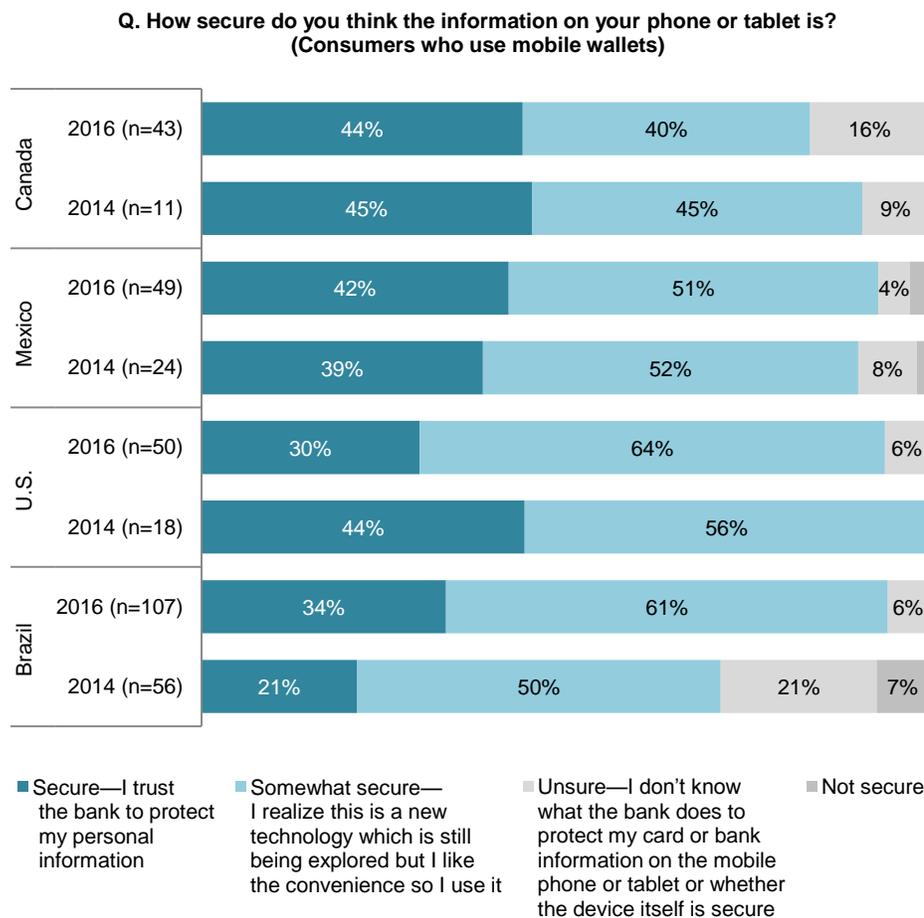
5. Ehsaan Ahmed, "The Rising Trend of Cashless Payments," Gulf News, published July 17, 2016, accessed October 10, 2016, <http://gulfnews.com/business/sectors/banking/the-rising-trend-of-cashless-payments-1.1863595>.

MOBILE WALLET SECURITY

Consumer perceptions of bank-based mobile wallet security vary across the globe, though in general consumers have a high degree of confidence in the security of mobile wallets. In most geographies surveyed, roughly 80% of consumers report being at least somewhat comfortable with mobile wallet security. In most cases, confidence in 2016 is similar to what it was in 2014, with the exceptions of Brazil, Mexico, and New Zealand, where it has increased statistically. It is notable that in 2014 a generally very small number of respondents used mobile wallets; that number increases in the 2016 survey, indicating greater adoption of mobile wallets among consumers.

In the Americas, high levels of confidence remained stable or increased. At first glance, it appears confidence decreased in the U.S. Due to the very small population using mobile wallets in 2014, this is not a statistically valid decrease. While there is variation across geographies, overall confidence across the region remains above 80% (Figure 6).

Figure 6: Perceptions of Mobile Wallet Data Security in the Americas

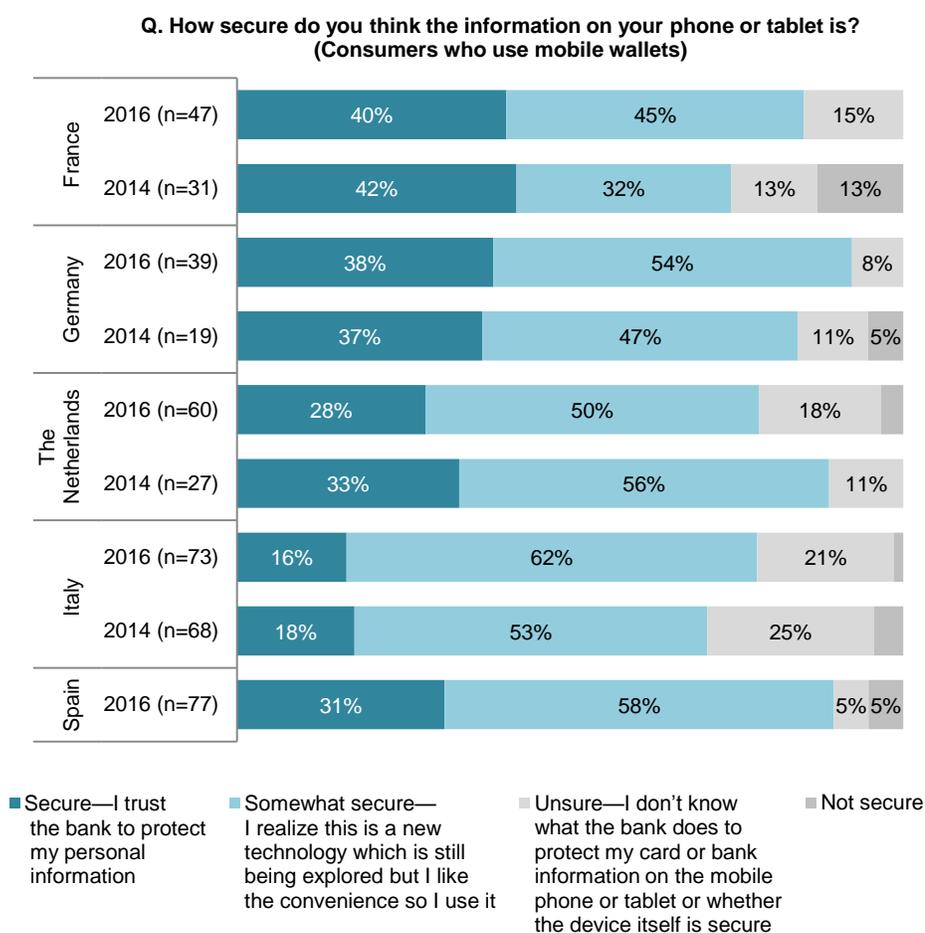


Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016 and Q1 2014

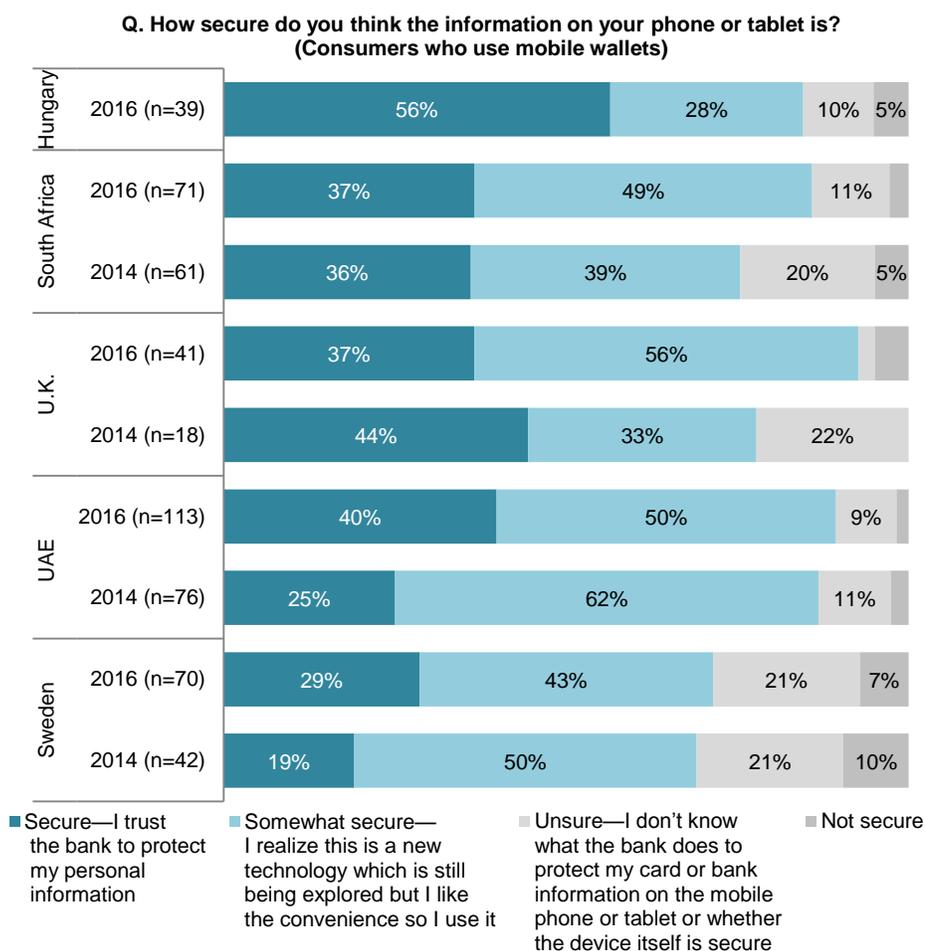
In EMEA, overall confidence remains generally high, though it varies noticeably across different countries and is often lower than in the Americas and the Asia-Pacific. There are noticeable, but not statistically significant, increases in confidence across the region with the exception of the Netherlands. Even there, the decrease in confidence is not statistically significant and is likely more representative of a larger sample size (more than double) than a dramatic decrease in overall consumer confidence.

Much like other regions, the EMEA experiences a complex interplay between mobile wallet adoption and consumer confidence—as more consumers adopt mobile wallets, the wallets become a bigger target for criminals. And more people will be exposed to fraud, driving down confidence, which in turn could negatively impact adoption in the future (Figure 7 and Figure 8).

Figure 7: Perceptions of Mobile Wallet Data Security in Eurozone



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016 and Q1 2014

Figure 8: Perceptions of Mobile Wallet Data Security in EMEA (Non-Eurozone)

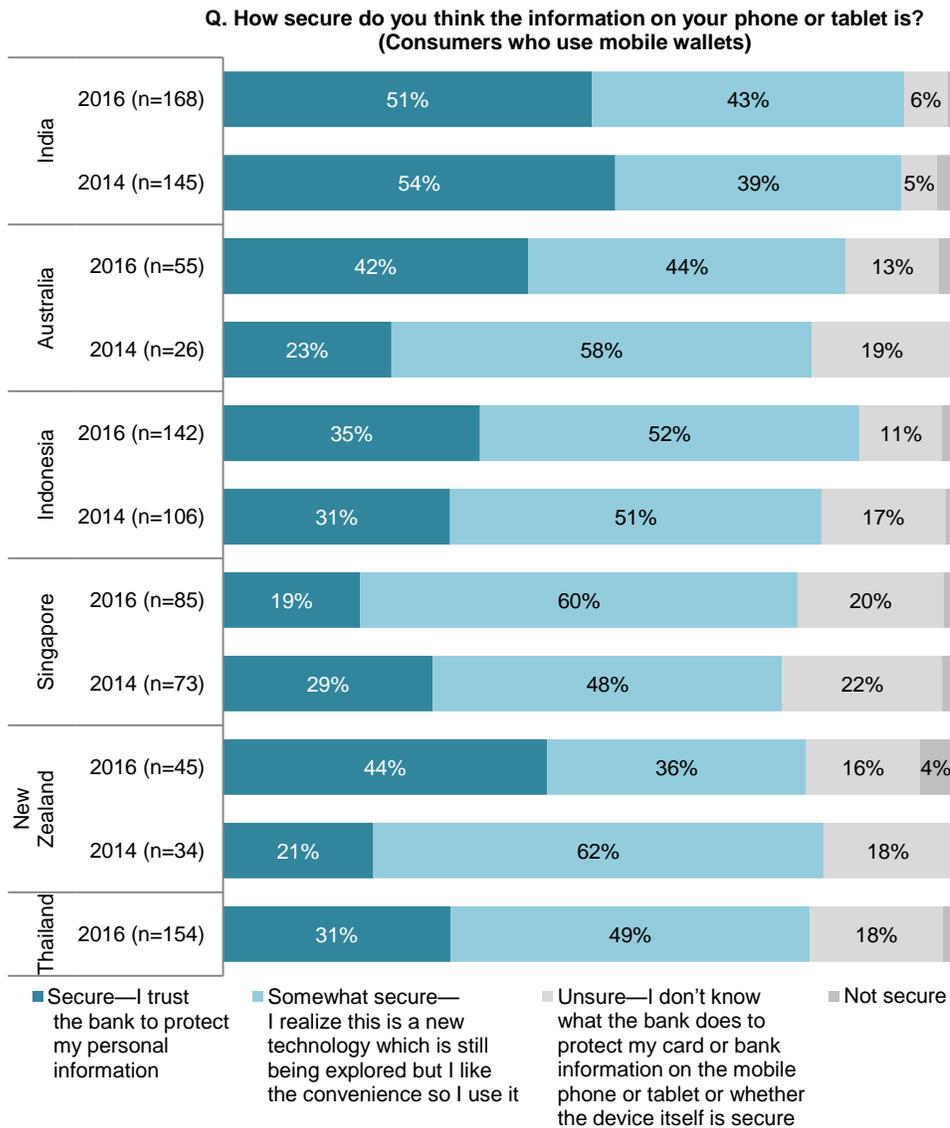
Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016 and Q1 2014

Consumer confidence with mobile wallets in the Asia-Pacific region shows more strong differences between countries than in the Americas or EMEA, but around 80% of consumers report they feel at least somewhat secure with mobile wallets. India is a standout, with over 90% of consumers reporting they feel at least somewhat secure.

New Zealand was the only standout with strong confidence that doubled since 2014. This may be due in part to “Mobile Device Rules & Standards,” published in 2014 by Payments NZ, which oversees New Zealand’s payments infrastructure.⁶ These standards are meant to protect consumers and businesses and may have an impact on consumer confidence (Figure 9).

6. “Mobile Device Rules & Standards,” Payments NZ, published May 14, 2014, accessed October 31, 2016, http://www.paymentsnz.co.nz/cms_show_download.php?id=108.

Figure 9: Perceptions of Mobile Wallet Data Security in the Asia-Pacific



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016 and Q1 2014

RETAILERS

Retail transactions are some of the most common and impactful transactions for consumers. The impacts for retailers are also substantial. If customers don't trust a retailer to protect their information, they will go somewhere else to make purchases. This applies to both in-person and online transactions covered below.

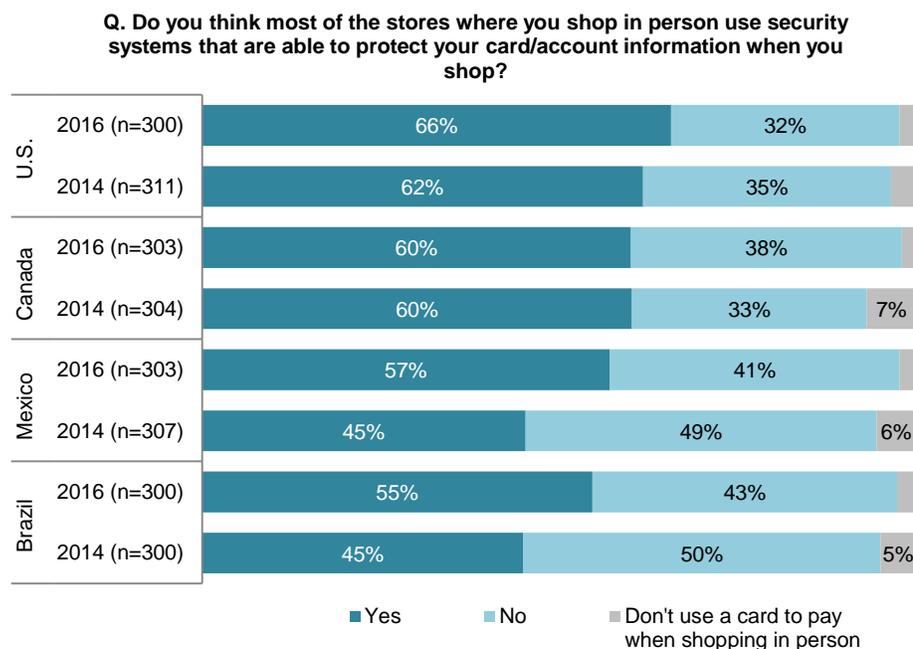
IN-PERSON SHOPPING

Many consumers indicate a lack of trust in stores where they shop in person to use security systems that adequately protect their card or account information. Part of this may be attributed to a number of very large and well-publicized retail breaches over the last few years, especially in the U.S. Consumers report less confidence in brick-and-mortar merchants' ability to protect payment information than they do in online merchants' abilities.

In general, across geographies, confidence has been rising compared to 2014. Some of the lowest confidence is found in fast-growing economies in South and Southeast Asia. Yet even here, confidence levels are quite high, with no country below 80% confidence.

Confidence levels that retailers protect customer data are relatively close across the Americas, ranging from 66% in the U.S. to 55% in Brazil, a statistically significant difference. Both Mexico and Brazil saw 10-point increases compared to 2014 results (Figure 10).

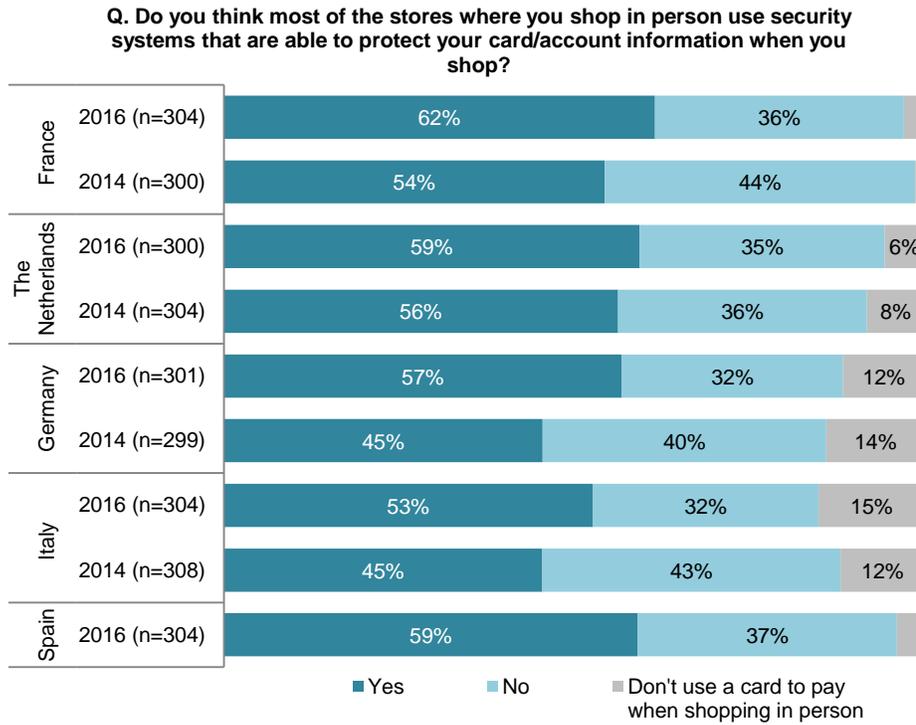
Figure 10: In-Person Shopping in the Americas



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016 and Q1 2014

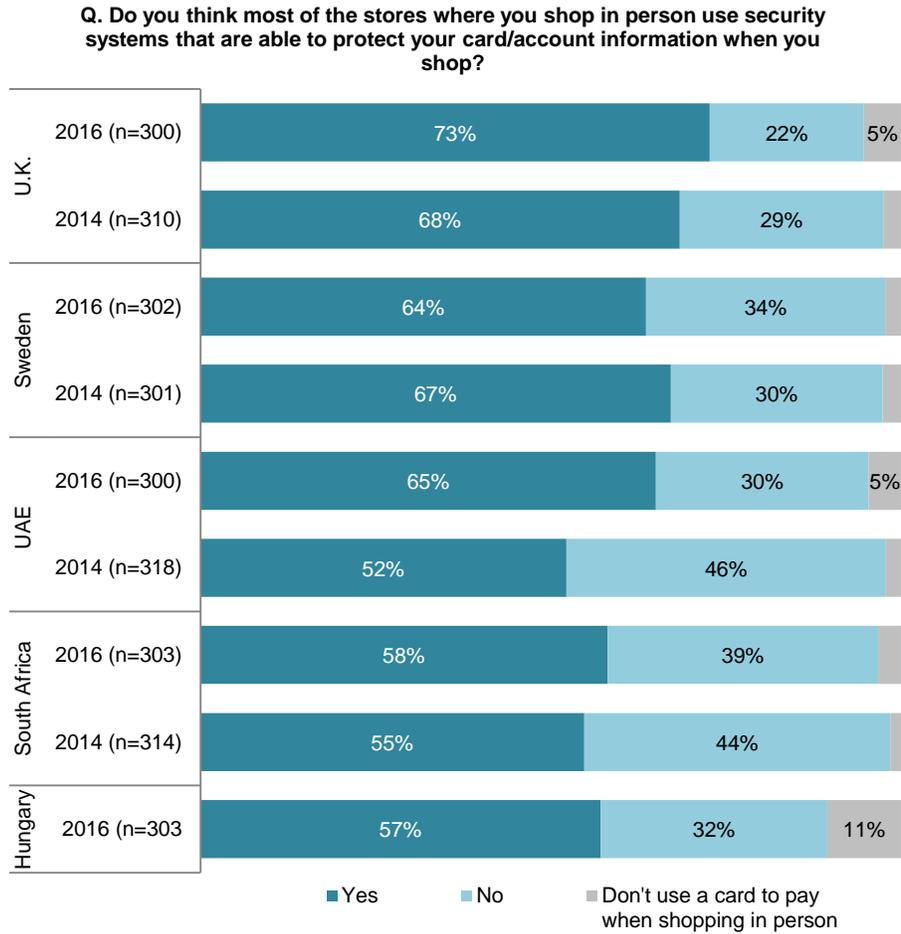
The confidence levels in EMEA vary more widely than in the Americas but still track in the 55% to 65% range in most countries. In some countries, such as Germany, Italy, and Hungary, larger portions of respondents report not using cards for in-person shopping (Figure 11 and Figure 12).

Figure 11: In-Person Shopping in Eurozone



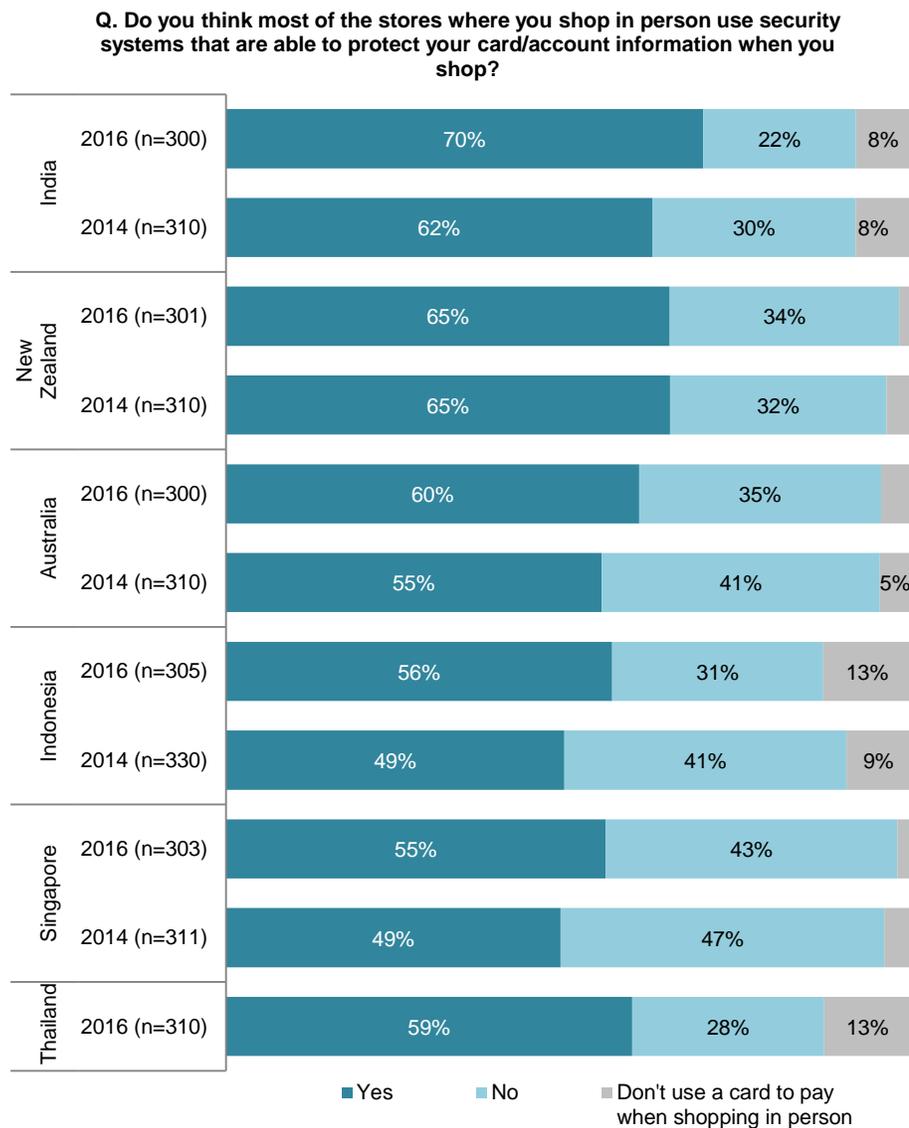
Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016 and Q1 2014

Figure 12: In-Person Shopping in EMEA (Non-Eurozone)



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016 and Q1 2014

The Asia-Pacific region tracks quite closely with the EMEA region in confidence. Indonesia and Thailand show the lowest rates of card usage for in-store purchases. This could be due to a number of factors, including high rates of mobile wallet use (Figure 5), lower payment card acceptance, and preference for cash in more rural areas (Figure 13).

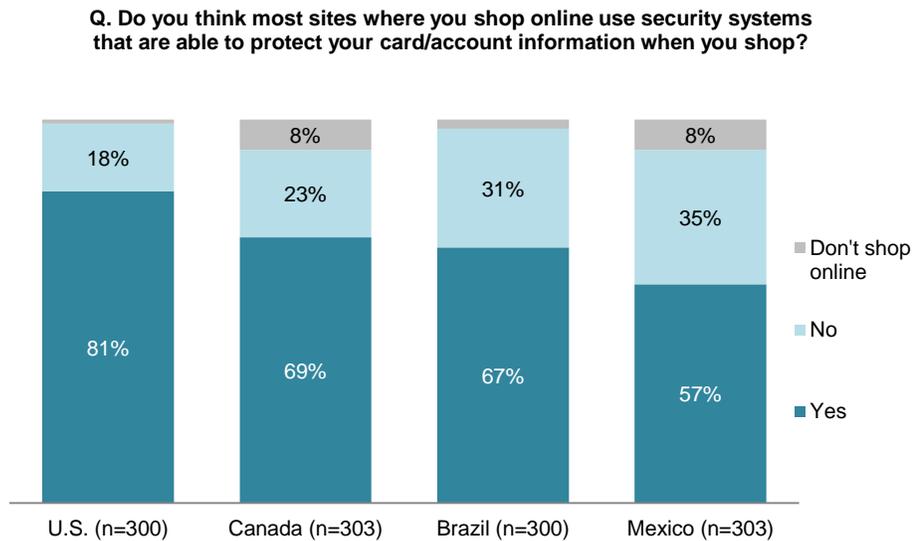
Figure 13: In-Person Shopping in the Asia-Pacific

Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016 and Q1 2014

ONLINE SHOPPING

Online shopping, and increasingly mobile online shopping, continues to be a critical channel for commerce. Consumer confidence in online merchants hinges on both security and convenience, which also help to gain repeat customers and minimize cart abandonment and chargebacks.

In the Americas, over half of all respondents believe sites at which they shop have security systems to protect their information, but the range was rather wide. In the U.S., 81% of respondents believe security measures are in place, while only 57% in Mexico respond the same way. This could be due to a longer tradition of online shopping in the U.S. and the marketing of security measures (Figure 14).

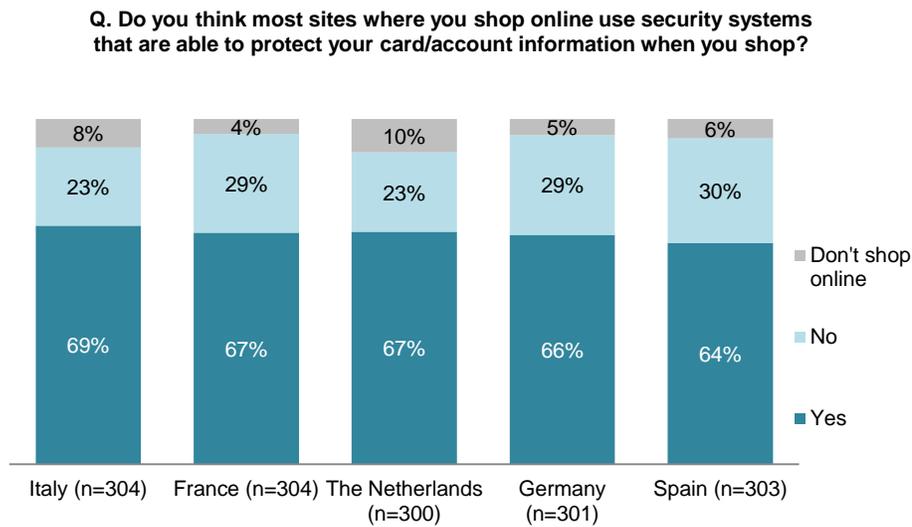
Figure 14: Online Merchant Security in the Americas

Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

EMEA shows more variation in both confidence and overall use of online shopping. Eurozone countries showed little variation across the five countries surveyed and are statistically the same. This is most likely due to harmonization of consumer protection and privacy laws and regulations across the EU. Outside of the eurozone countries, there was far more variation, with the U.K. providing responses similar to the U.S. and Sweden responding similarly to the eurozone countries surveyed.

Respondents in South Africa and Hungary report the lowest rates of online shopping, with 15% and 16%, respectively, reporting they do not shop online. This could represent less maturity in the online shopping market in these countries and, anecdotally, less confidence in online shopping (Figure 15 and Figure 16).

Figure 15: Online Merchant Security in Eurozone



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

Figure 16: Online Merchant Security in EMEA (Non-Eurozone)



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

Respondents in the Asia-Pacific region showed significant variation. In India, 77% respond that security systems are in place, and in Singapore, only 51% report the same. Consumer perceptions in Singapore may be impacted by a large migrant worker population and generally less online shopping compared to other regions. New Zealand and Australia, while 10 percentage points apart, track closely with the eurozone countries surveyed (Figure 17).

Figure 17: Online Merchant Security in the Asia-Pacific



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

FRAUD AND DATA BREACHES

Consumers in the U.S. are far more forgiving toward merchants that cause them to experience fraud or a data breach. The U.S. is the only country surveyed where less than half of consumers would stop shopping at such a merchant. There was a very broad range of reactions to this query across the Americas, with 86% of consumers in Brazil and 84% in Mexico saying they would stop shopping with a merchant or retailer if they experienced fraud or a data breach associated with the entity (Figure 18).

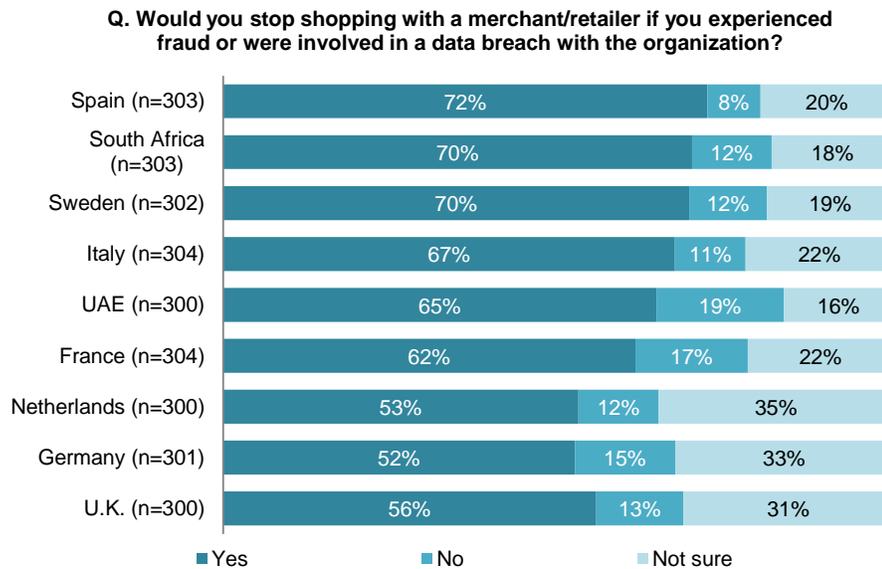
Figure 18: Stop Shopping in the Americas



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

The majority of consumers in EMEA state they would stop shopping at a merchant or retailer that allowed fraud to occur or involved them in a data breach. These figures are very high, ranging from 52% to 72%; if consumers actually did stop shopping when these events occurred, merchants and retailers would have to invest in better data security and fraud prevention solutions (Figure 19).

Figure 19: Stop Shopping in EMEA



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

Last, consumers in the Asia-Pacific react in a similarly severe manner over the prospect of a retailer or merchant allowing fraud to occur on their account or their data to be breached (Figure 20).

Figure 20: Stop Shopping in the Asia-Pacific

Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

Across all 20 countries, an average of 65% of consumers surveyed state that a fraud experience or data breach would cause them to stop shopping with the merchant or retailer that enabled that incident.

STORED DATA

Storing and managing personal data has become more critical than ever before for every type of firm. Data breaches and hacking attempts have become incredibly common. Making matters worse, a breach or hack at one firm can impact other firms, especially as many people reuse usernames and passwords.

Different countries have different sets of data security and privacy laws, regulations, and industry standards for data protection. This can be very confusing for firms large and small, and certainly for consumers who regularly see news of hacking and data breaches across mass media on a regular basis.

Across all the countries surveyed, only three—the U.S., India, and Thailand—had over 50% of respondents indicate that they trust businesses to protect their personal data, and by statistically small margins. This reflects the reality that for many years, firms' ability to protect data has lagged behind criminals' ability to collect and monetize the data.

In the Americas, respondents from the U.S. showed one of the highest levels of trust out of all countries surveyed, with 54% responding that they trust firms to protect their data. This is surprising considering the frequent news about breaches and hacks. With the exception of respondents from Mexico, the number of respondents who report they are unsure of data protections and those who report they do not trust firms' data protection tend to be about the same and total over half of the responses. Respondents from Mexico much more strongly respond that they do not trust firms (Figure 21).

Figure 21: Security of Stored Data in the Americas



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

In EMEA, the respondents tend much more toward an “unsure” response when asked whether they trust firms to protect their data. This is in some ways surprising, especially in the EU, where there are more strict data privacy and security protections than in many parts of the world, in particular the U.S. This is even more surprising in Germany, which has some of the strictest data protection laws and regulations in the world.

In general, European consumers are much more aware and conscious of data protection and privacy compared to their counterparts in other parts of the world, yet the number of respondents who say they are unsure of firms’ ability to protect their data suggests there is a lack of clarity and communication about how data is stored, managed, and protected. No country in the EMEA region reports over 49% of respondents indicating they trust firms to protect their data (Figure 22 and Figure 23).

Figure 22: Security of Stored Data in Eurozone



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

Figure 23: Security of Stored Data in EMEA (Non-Eurozone)

Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

Similar to their responses about how well online merchants protect information, respondents show significant variation in the Asia-Pacific region, with 60% of those in India responding they trust firms with data, and only 36% in Singapore saying the same. In general, the perception of firms' data security tracked very closely with the perception of merchant security capabilities.

A large minority of respondents across the region report they are unsure whether they trust firms to protect their data. Singapore is a surprising outlier, considering its strong regulations regarding data protection and governance. In general, consumers in Singapore do much less online shopping than do those in many other geographies due to the relatively small size of the country and the ease of access to brick-and-mortar stores (Figure 24).

Figure 24: Security of Stored Data in the Asia-Pacific



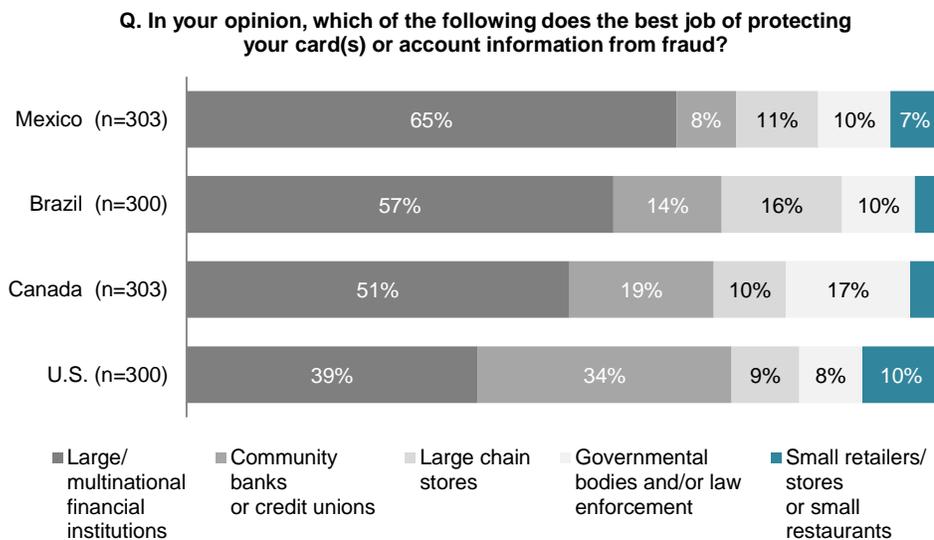
Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

Even though data breaches have been common, consumer confidence in merchants’ ability to protect personal information increased to 43% in 2016 from 34% in 2014, among the 17 countries surveyed in both studies.

PROTECTING CARD AND ACCOUNT INFORMATION

When asked about what types of organizations best protect consumer information from fraud, respondents in Mexico and Brazil have higher levels of confidence in large financial institutions—65% and 57%, respectively—than in other types of institutions. In the U.S., there is a nearly even split between large financial institutions and community banks and credit unions, at 39% and 34%, respectively. This may be due to much more national news coverage when an incident occurs with a large financial institution compared to more local coverage when it comes to community banks and credit unions (Figure 25).

Figure 25: Best Data Protectors in the Americas

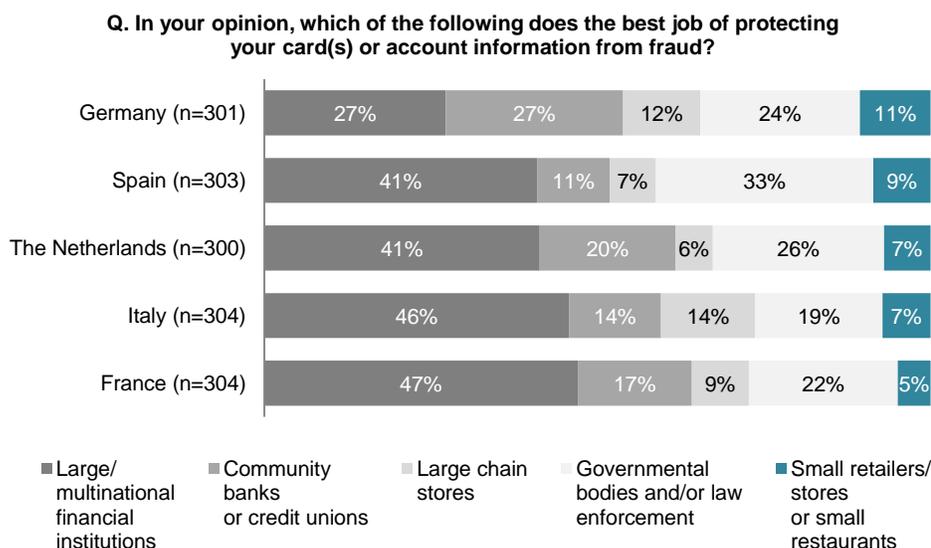


Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

There is variation in perception across EMEA as to which organizations best protect customer information. In the eurozone nations surveyed, large multinational financial institutions and governments ranked the highest, most likely due to generally strong data protection laws and regulations. Non-eurozone countries surveyed showed much greater variance, with 59% of respondents in South Africa viewing large multinational financial institutions as the most reliable, whereas only 19% in Sweden felt the same. In Germany, perception was nearly evenly split between multinational financial institutions, the government, and community banks and credit unions.

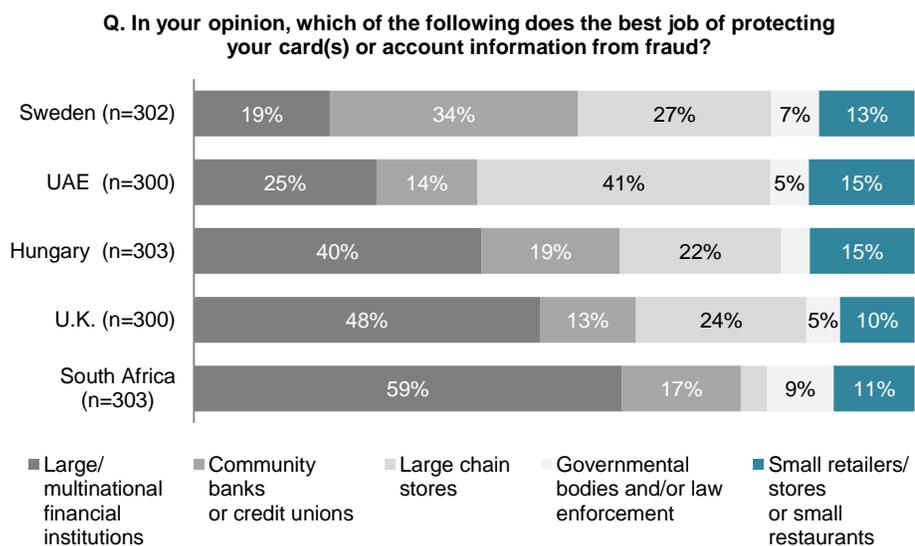
Large chain stores outside of the eurozone generally showed stronger consumer confidence than much of the rest of the world, with the notable exception of South Africa. The UAE distinctly stands out with strong positive perceptions of large chain retailers (Figure 26 and Figure 27).

Figure 26: Best Data Protectors in Eurozone



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

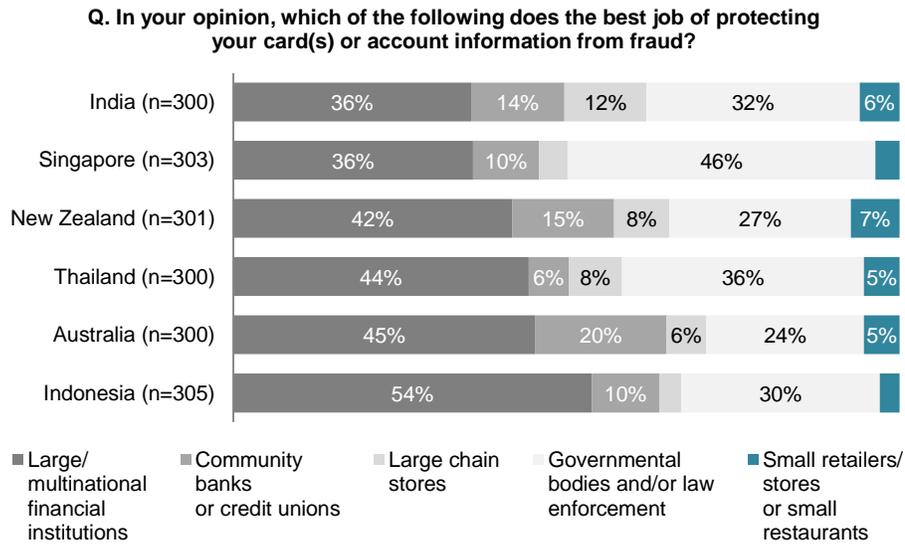
Figure 27: Best Data Protectors in EMEA (Non-Eurozone)



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

In the Asia-Pacific region, there are more differences between countries than in some other geographies. Large multinational financial institutions and, in some cases—notably Singapore—governments are highly trusted when it comes to data protection. In Singapore, the government’s efforts for strong data protection policies appear to have a real impact on consumer perception. In other countries in the region, large financial institutions appear to be generally well-trusted, likely due to strong brand image and efforts to promote consumer confidence (Figure 28).

Figure 28: Best Data Protectors in the Asia-Pacific



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

CONSUMER FRAUD CONCERNS

Consumers clearly have an interest in security and have concerns about how merchants and other organizations they interact with protect their data and protect them from fraud. Combating fraud and improving security require a partnership between businesses and consumers to succeed. Across the range of countries surveyed, the standout fraud concern is theft by computer hacking. This reflects the concerns consumers have about how their data is protected by merchants.

Conversely, across all regions, very few are concerned about shopping or paying bills using their phones or tablets. This may be attributed to a few possible factors:

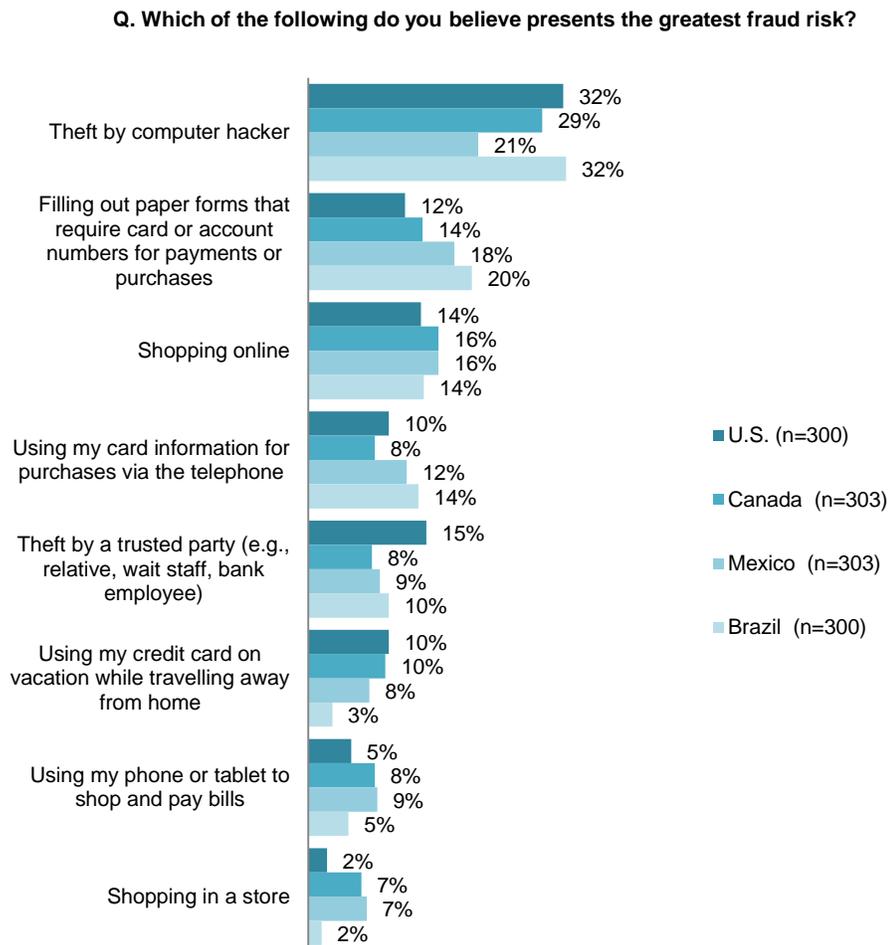
- Many consumers view their mobile devices and tablets as very different from laptops and desktops. While they are certainly different, they are all computers in different form factors, and they all have potential vulnerabilities. This misperception may lead consumers to be less concerned with security when it comes to mobile devices. It is important to remember that NASA sent men to the moon with a fraction of the computing power now available in a watch.
- Consumers may not have experienced fraud through their mobile phones and tablets yet. One single Android exploit, Stagefright, was detected on as many as 1,800 devices per day in late 2015.⁷ While the amount of mobile malware is growing, many consumers may not have experienced it yet or may not have been able to connect a mobile event to an actual fraud.
- The concept of “computer hacking” is not particularly well-defined in consumers’ minds and may be perceived as more focused on businesses and governments than on personal devices.

Though most of the regions’ respondents show similar patterns, there are some interesting differences between some countries.

In the Americas, filling out paper forms requiring account information is a similar concern across all countries surveyed, reflecting a worry that such paper forms might be used for fraudulent purposes due to poor care exercised by the custodians of those documents.

It also seems that across the Americas region, consumers underestimate, or underreport, the risk of theft by a trusted party (Figure 29).

7. Bruce Snell, “Mobile Threat Report: What’s on the Horizon for 2016,” Intel Security and McAfee, published March 1, 2016, accessed September 18, 2016, <http://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf>.

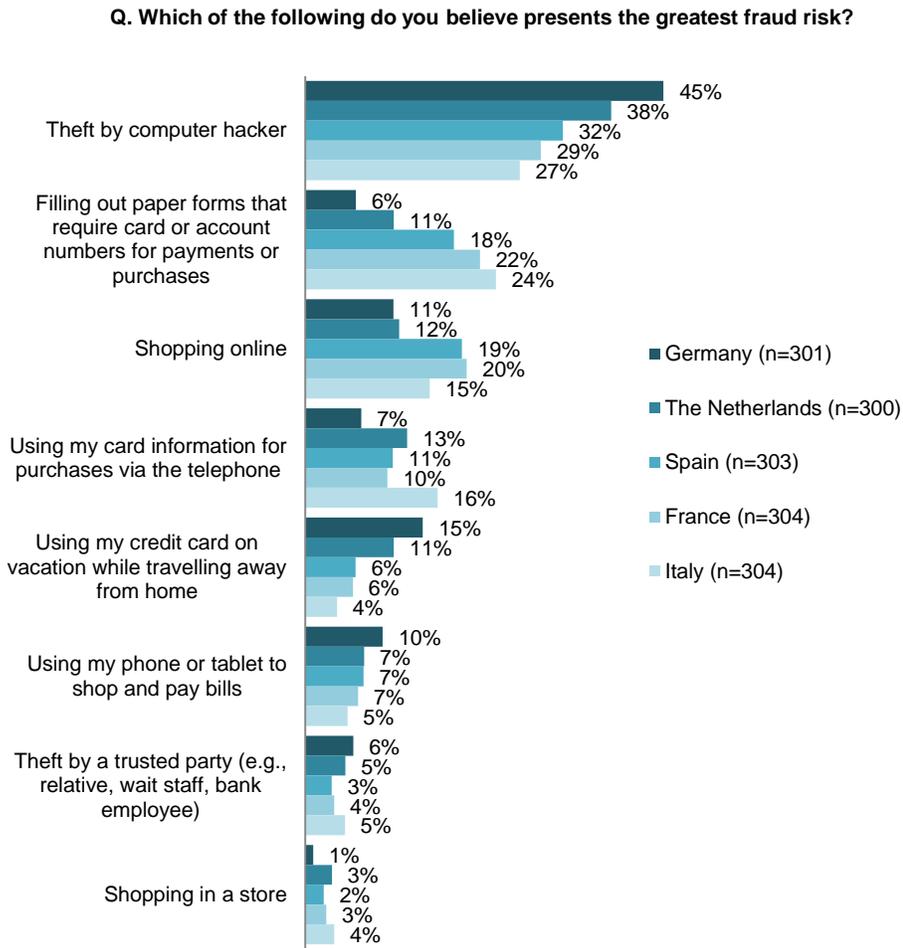
Figure 29: Greatest Fraud Risks in the Americas

Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

Patterns in the EMEA region broadly reflect the rest of the world, again with some interesting differences. Germany offers an interesting example in which 45% of consumers report theft by computer hacker as the greatest risk, higher than every other country surveyed in the region. The low level of concern regarding in-store shopping does not necessarily reflect consumers' attitudes toward the ability of merchants to protect consumer data.

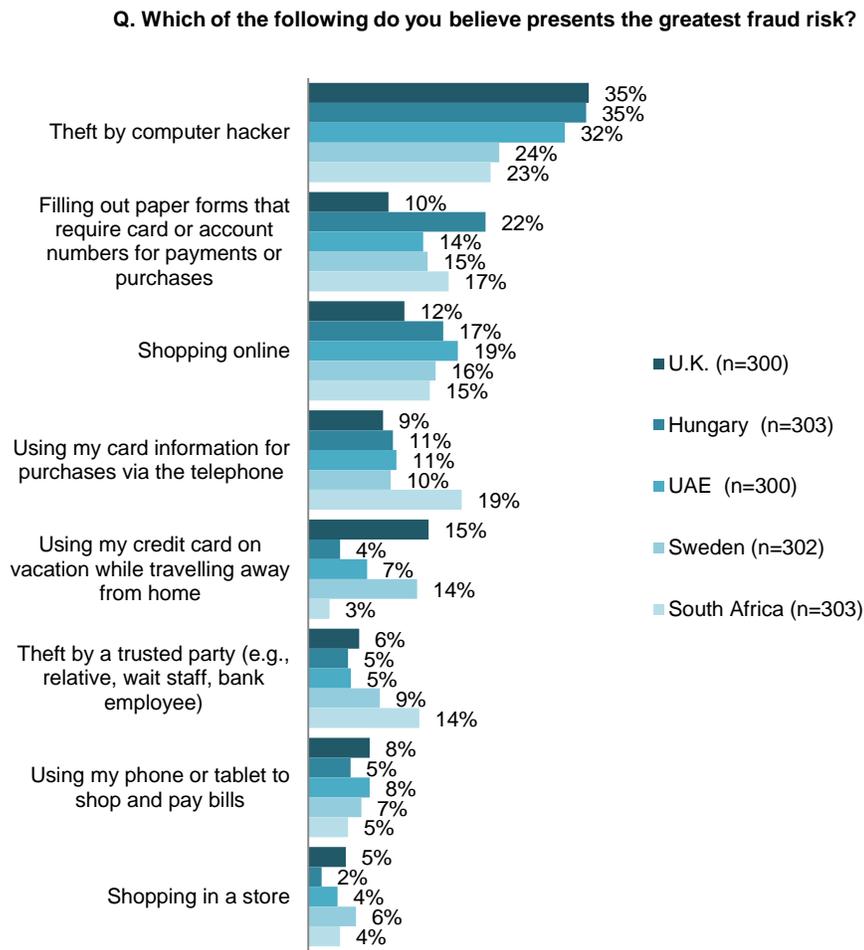
Another standout is greater concern from consumers in Hungary, France, and Italy regarding personal data available on paper forms. Much like in the Americas, this could be attributed to general distrust in the custodianship of those forms as well as consumers' perception of such information's usefulness in perpetrating fraud. On this metric, Germany was one of the lowest in fraud concern (Figure 30 and Figure 31).

Figure 30: Greatest Fraud Risks in Eurozone



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

Figure 31: Greatest Fraud Risks in EMEA (Non-Eurozone)

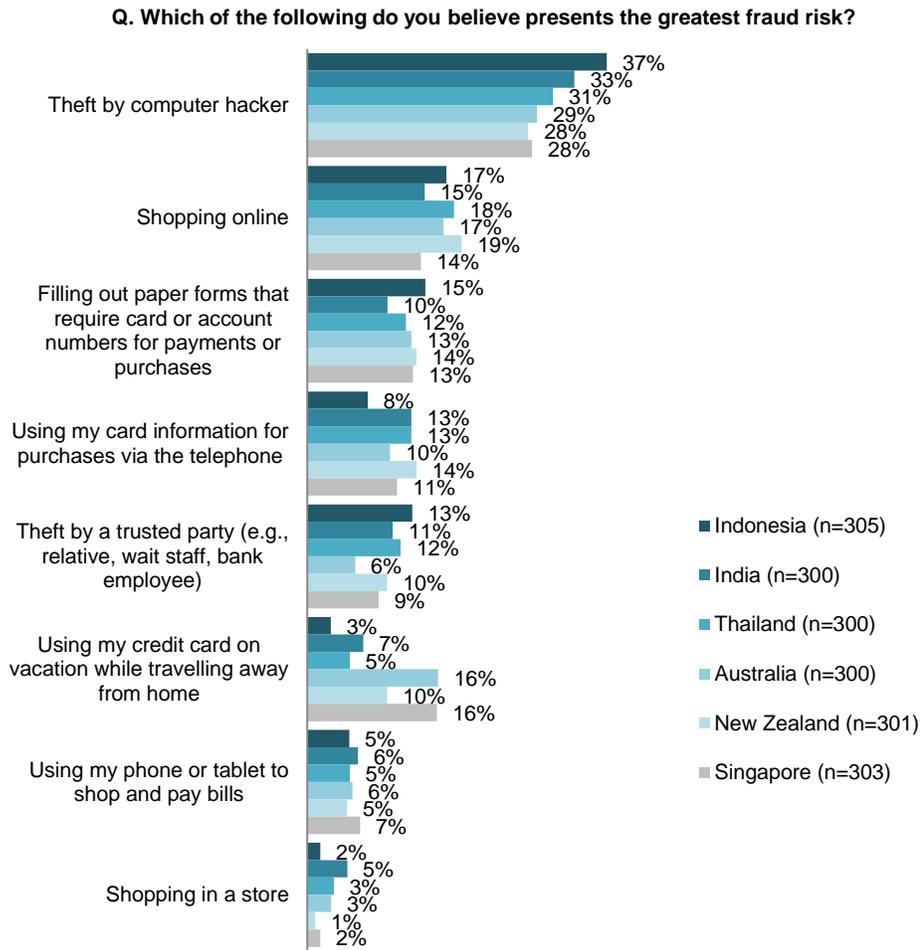


Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

As with the other regions, the general top concern in the Asia-Pacific region is theft by computer hacking. Like other regions, there are some interesting cases. Concern about credit card use while traveling is statistically higher among respondents from Australia and Singapore than among those in Thailand and Indonesia, and is similar to the other countries in the region as well as to respondents in the U.K., Germany, and the U.S.

Similar to the EMEA region, the generally low concern regarding in-store purchases does not appear to reflect the modest level of confidence consumers report in merchants’ ability to protect their data. This can also be reflective of consumers’ broader view of “computer hacking,” which covers a broad range of events that may or may not include in-store data breaches due to hacking (Figure 32).

Figure 32: Greatest Fraud Risks in the Asia-Pacific



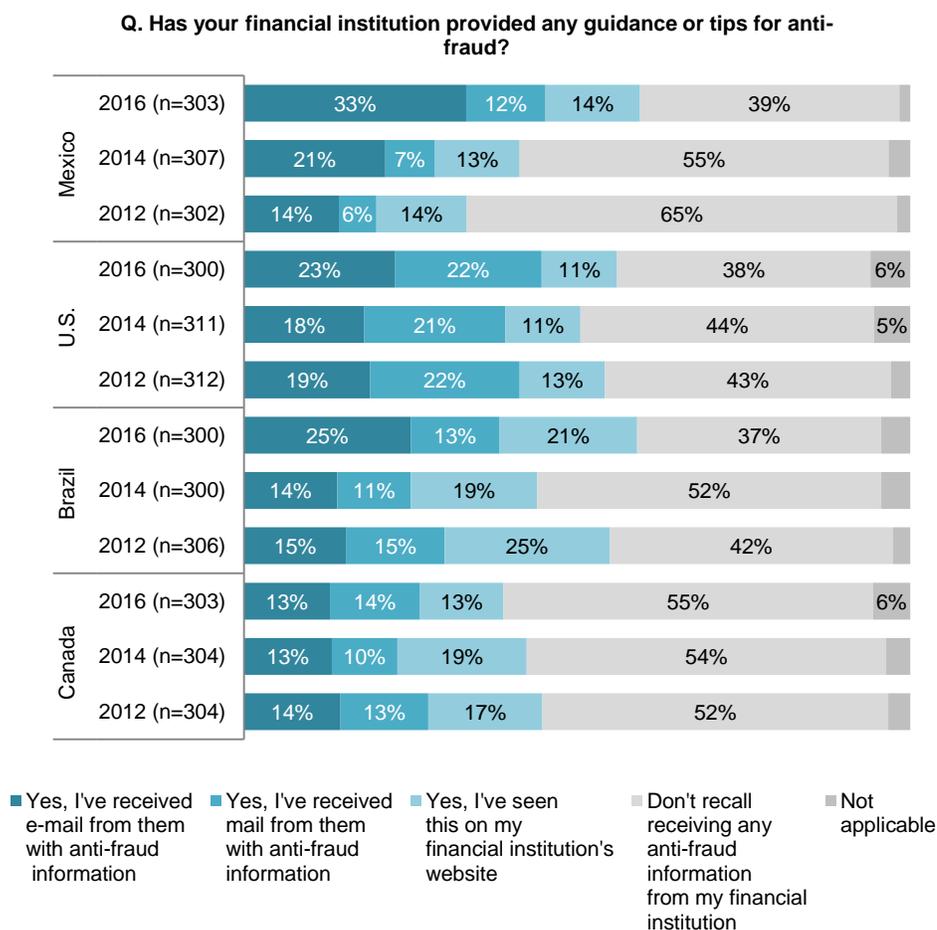
Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

FRAUD EDUCATION

Consumer education on fraud awareness varies significantly across and within regions. Mexico and Brazil show an improved recognition of anti-fraud education by financial institutions than in earlier years; in the U.S. and Canada, levels are similar to prior years. It is concerning that in 2016 in every country in the Americas surveyed, over one-third of consumers could not recall anti-fraud guidance coming from their financial institutions.

How well consumers are educated about fraud clearly correlates with how likely they are to become victims of fraud.⁸ Mexico shows the greatest improvements in fraud education, while Canada has shown consistently low numbers going back to 2012. This region has an opportunity to improve customer messaging and communication with respect to avoiding fraud (Figure 33).

Figure 33: Fraud Education in the Americas



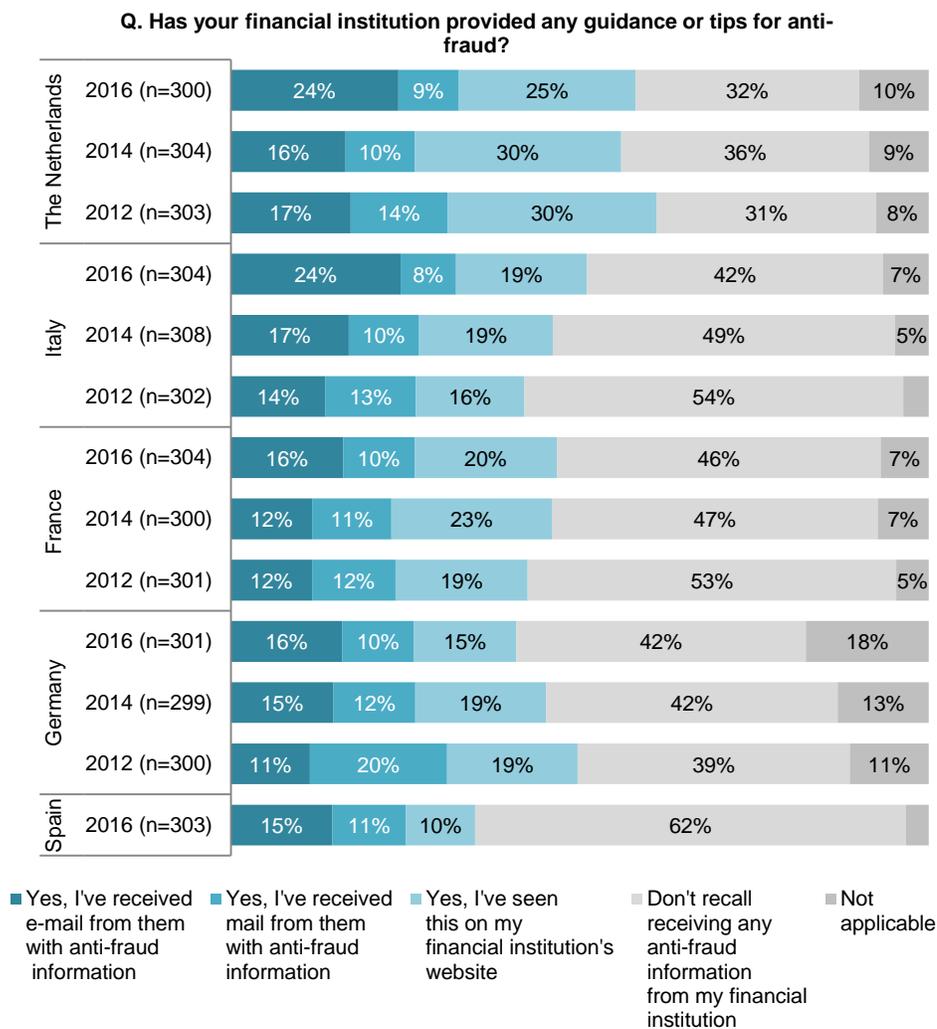
Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

8. See Aite Group's report *2016 Global Consumer Card Fraud: Where Card Fraud Is Coming From*, July 2016.

In EMEA nations, there is somewhat less year-over-year fluctuation compared to the Americas, but still at least one-third of consumers report they don't recall receiving any anti-fraud education or messaging. This results in a higher risk of fraud for a large group of consumers.

Financial institutions can help improve their image by communicating clearly how they work to protect consumers from fraud without giving up so much information that criminals can use it to their advantage. This can improve customer trust and confidence while helping to reduce fraud losses (Figure 34).

Figure 34: Fraud Education in Eurozone

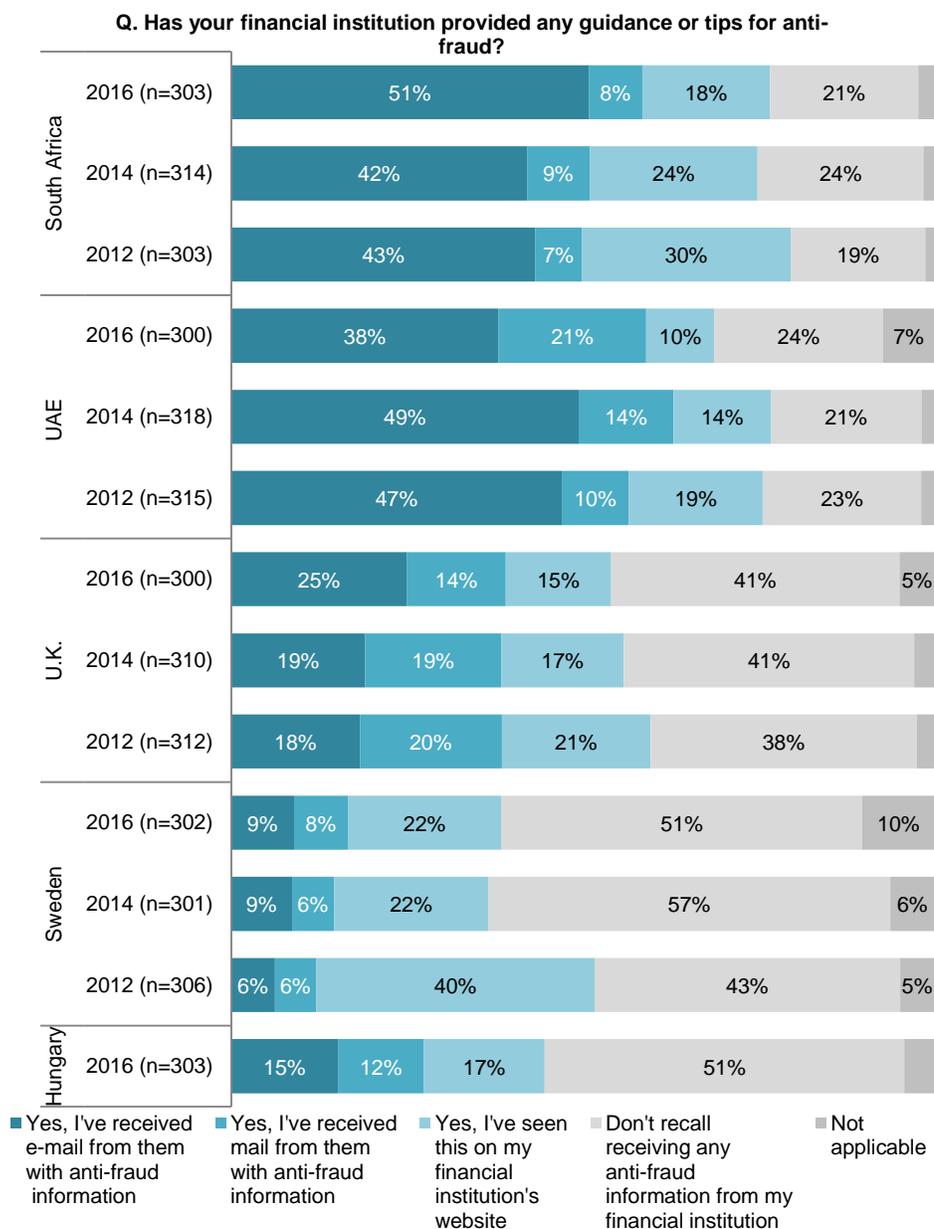


Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

Non-eurozone parts of EMEA show more variety in customer perception, with countries such as South Africa and the UAE showing much higher levels of consumer education—almost three-quarters of respondents report that they have received guidance from financial institutions. This compares to Sweden and Hungary, where less than 50% of respondents recall anti-fraud

information. The U.K. tracks much more closely with the U.S. and eurozone countries, but still just over 50% of respondents recall anti-fraud messaging (Figure 35).

Figure 35: Fraud Education in EMEA (Non-Eurozone)

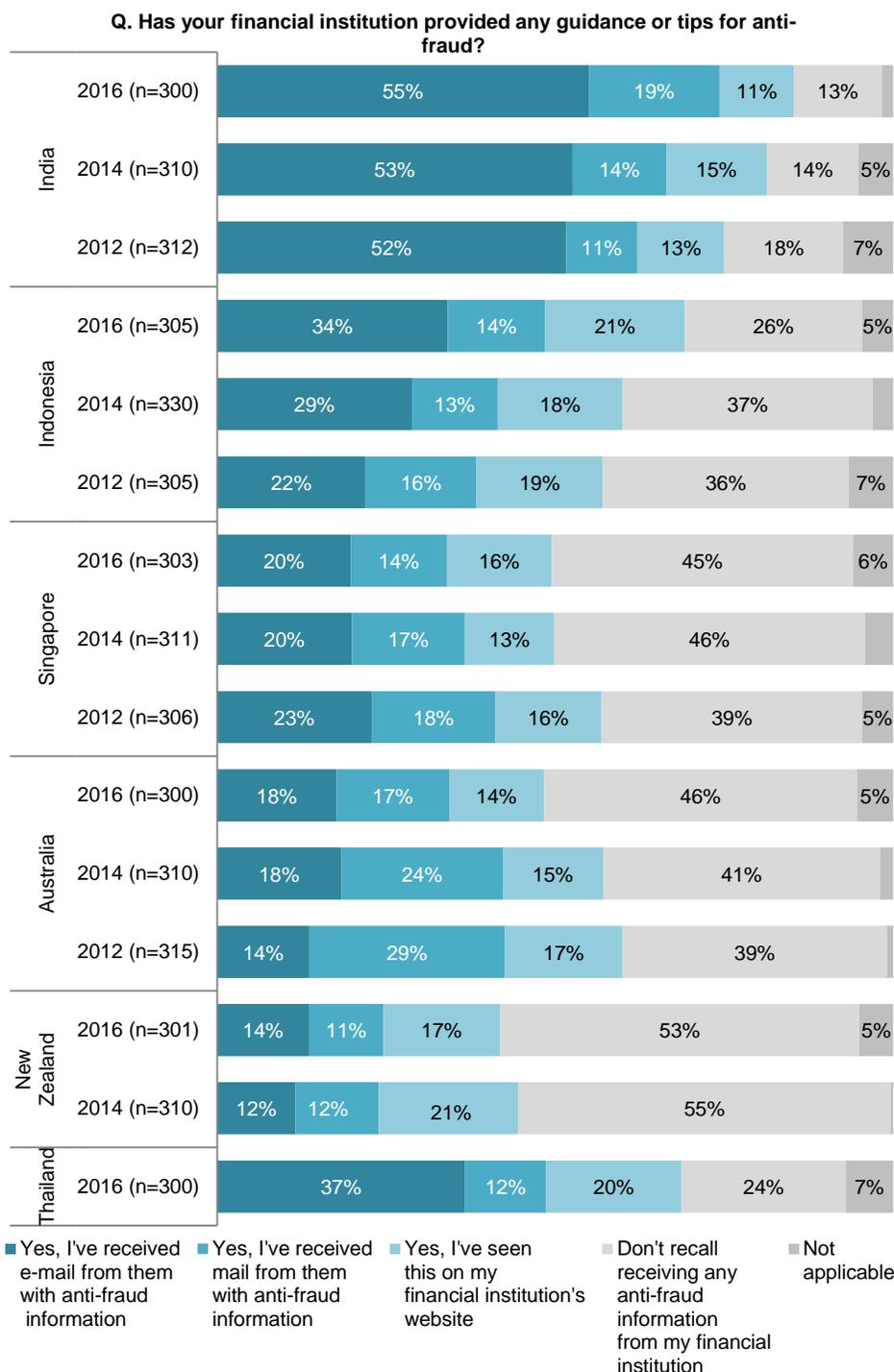


Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016 and Q1 2014, and in 17 countries, Q3 2012

Respondents in the Asia-Pacific region had a rather wide range of responses, with respondents in India, Indonesia, and Thailand reporting high levels of anti-fraud messaging compared to many other countries surveyed. Singapore, Australia, and New Zealand showed much lower levels of awareness of anti-fraud messages, with less than 50% of respondents in each country reporting they have seen some sort of anti-fraud education for 2016. Even though many institutions have

some form of anti-fraud education and training, it does not always seem to resonate with consumers (Figure 36).

Figure 36: Fraud Education in the Asia-Pacific



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016 and Q1 2014, and in 17 countries, Q3 2012

CONSUMER RESPONSE TO FRAUD ALERTS

Consumers are an integral piece of the fraud management puzzle. Whether they are reporting fraud or responding to alerts, consumers are critical to the process. The way in which financial institutions manage a consumer's fraud experience can have a significant impact on future decisions for those consumers. Meeting consumer expectations enables financial institutions to develop stronger relationships with customers and improve revenue.

In the Americas, the majority of consumers report they would prefer institutions to block transactions until they respond to the alert. In the U.S. and Canada, more consumers report they would prefer more granularity by allowing common transactions to be approved based on past purchase history, with 29% of Canadian consumers and 35% of U.S. consumers preferring this option. This is much higher than numbers reported in Brazil and Mexico, possibly due to lower awareness that this option is even possible.

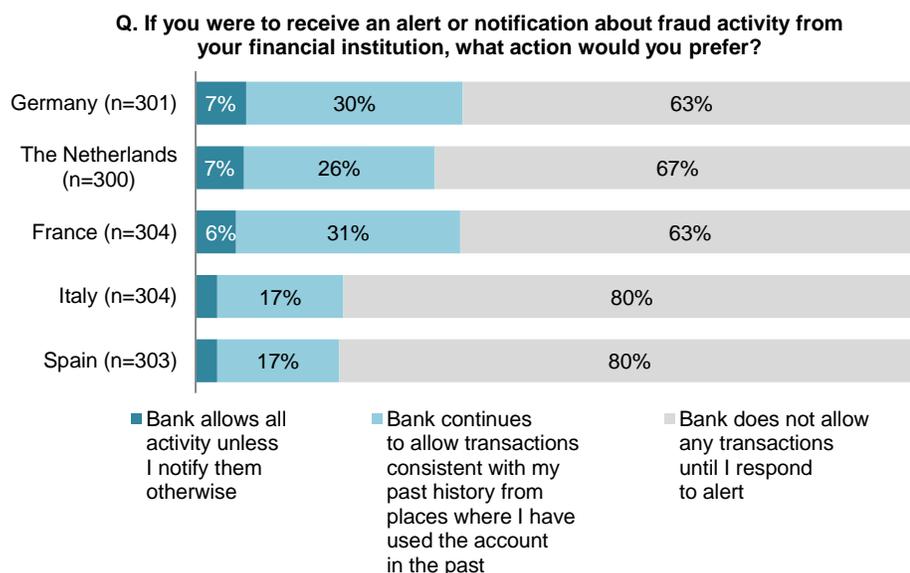
Tellingly, very few consumers in any of the geographies surveyed indicate they would like all transactions to be approved after an alert. This suggests that consumers have a good understanding of the impacts of card fraud and the need to work through some inconvenience to reduce fraud (Figure 37).

Figure 37: Actions Following Suspicious Activity in the Americas

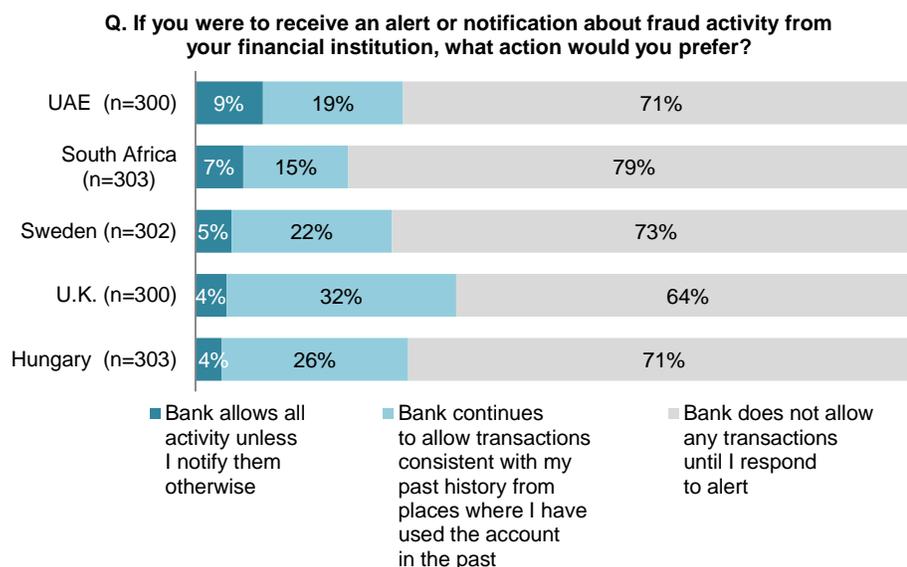


Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

Results in EMEA were generally quite similar to those for the Americas, with the majority of consumers in all countries preferring that banks block transactions until they respond to the alerts. Some consumers have a preference for allowing “common” historical transactions to be allowed while blocking other transactions, with responses ranging from 15% to 32% of consumers preferring this option. Only a small fraction of respondents, 3% to 9%, indicate they would prefer all transactions to be approved (Figure 38 and Figure 39).

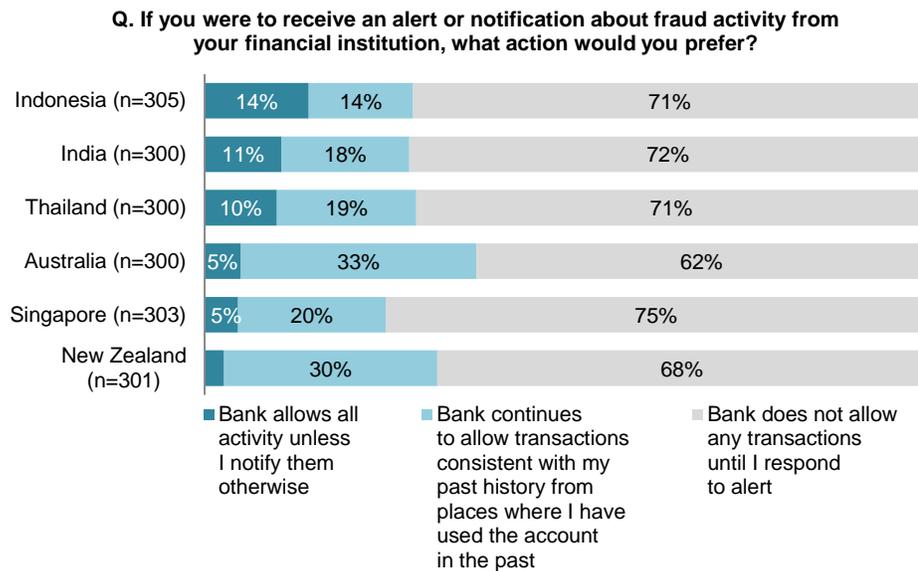
Figure 38: Actions Following Suspicious Activity in Eurozone

Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

Figure 39: Actions Following Suspicious Activity in EMEA (Non-Eurozone)

Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

Countries surveyed in the Asia-Pacific region show some variation between countries similar to that of EMEA or the Americas. A strong majority of consumers prefer transactions be blocked until they respond to the bank. Indonesian respondents stand out, with the largest number of respondents preferring all activity be approved unless they notify the bank (Figure 40).

Figure 40: Actions Following Suspicious Activity in the Asia-Pacific

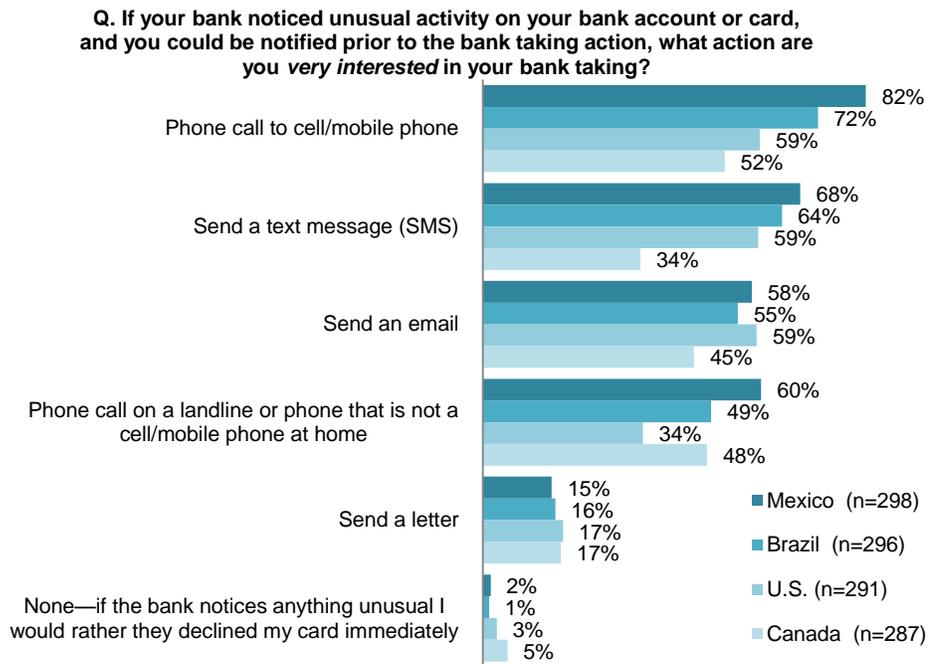
Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

Clearly, consumers are willing to be involved in preventing fraud, and institutions have a variety of methods to reach customers—some are more preferred than others. In general, consumers across all geographies prefer phone calls, with electronic options such as email and SMS following close behind. In almost every country surveyed, a significant minority of respondents include a physical letter as one of their preferred methods of contact.

The survey did not include a separate option for mobile application push alerts. This has become another convenient electronic option to both notify consumers and allow them to approve or reject transactions. Other newer communication methods, such as WeChat, were also not included.

Approximately half of respondents in Mexico, Canada, and Brazil report they would prefer to be contacted on a landline, and one-third in the U.S. report this as a preference. This may be reflective of the large number of U.S. consumers that have abandoned landline phones at home (Figure 41).

Figure 41: Contact Preferences in the Americas

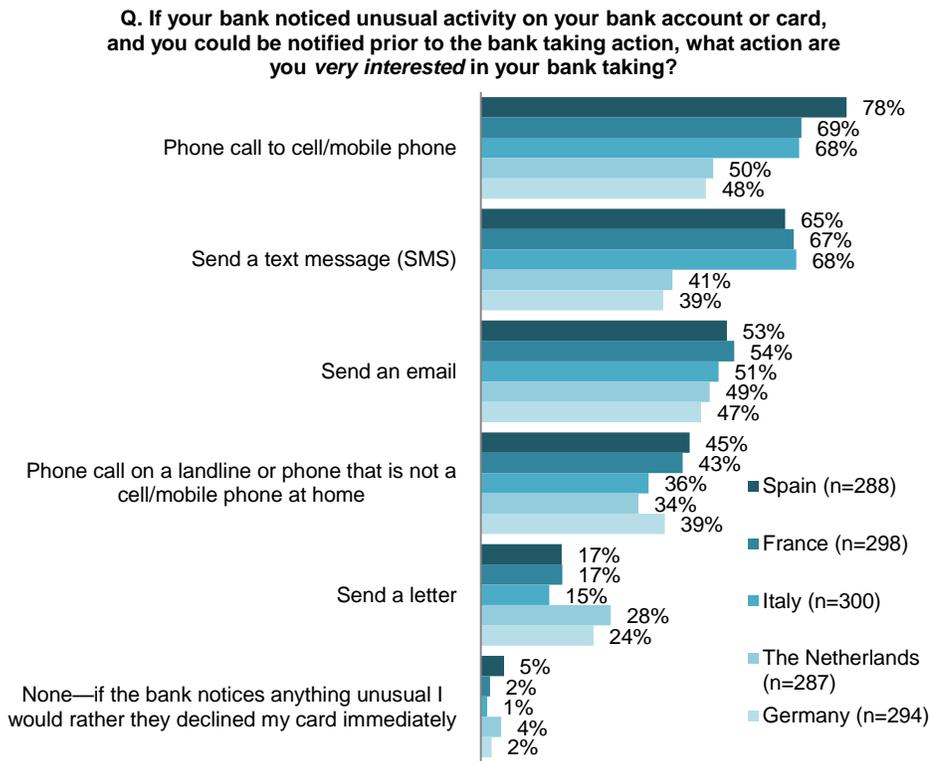


Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

Preferences in EMEA similarly skewed strongly toward calls to a mobile phone, followed by SMS and email alerts. Much like the Americas, between one-third and one-half of respondents show a preference for a phone call to a landline. Even so, it is clear that mobile-based communication is generally the strong preference across EMEA.

In several geographies within EMEA, respondents also expressed a desire for a physical letter. This does not imply that a letter would be the only form of communication, but it appears to be one of the forms of communication consumers appreciate (Figure 42 and Figure 43).

Figure 42: Contact Preferences in Eurozone



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

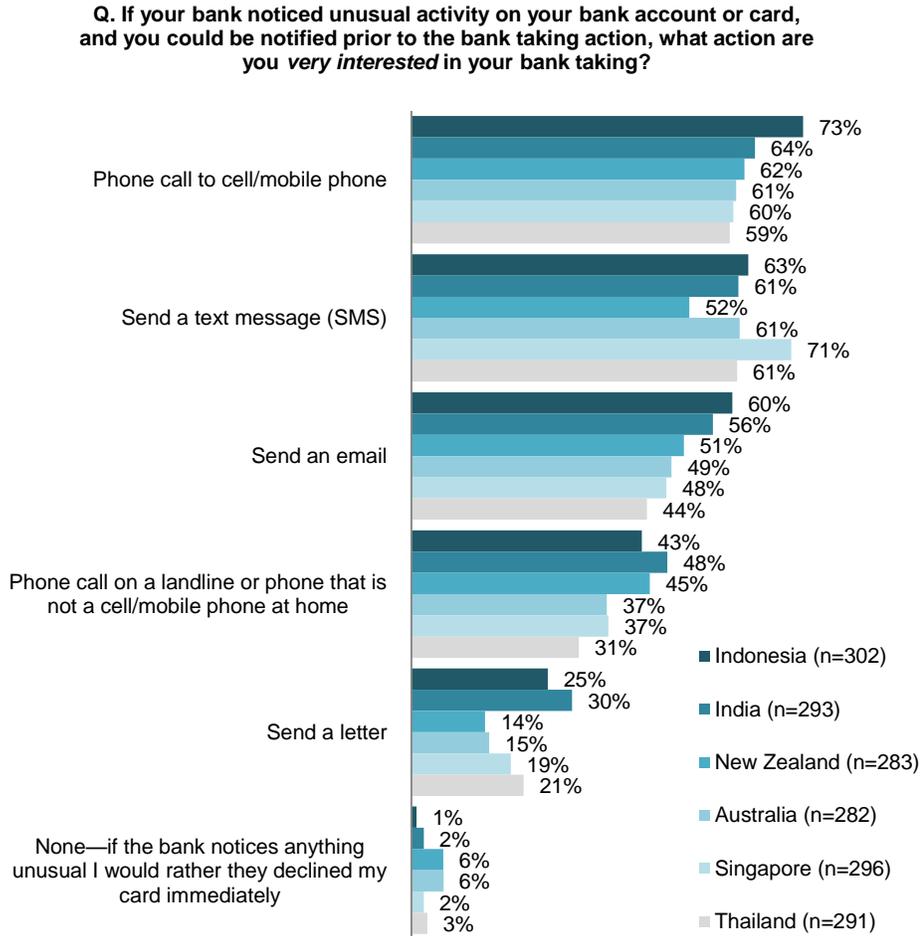
Figure 43: Contact Preferences in EMEA (Non-Eurozone)



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

Similar to the other regions, mobile-based communications, either SMS or calls to a mobile phone, were the most preferred in the Asia-Pacific region, with email coming in third. Much like EMEA, about one-third to one-half of respondents showed a preference for a landline phone call (Figure 44).

Figure 44: Contact Preferences in the Asia-Pacific



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016

Most consumers rarely leave home without their mobile devices, and consumers love the convenience of using them. Indeed, across all 20 countries surveyed, 75% of consumers indicate they are very interested in receiving a call to their mobile device or having an SMS message sent to their mobile device to partner with their financial institutions in preventing fraud.

CONCLUSION

Consumers share a number of concerns about how their personal information is protected and how businesses value data security and privacy. Consumers also show an interest in minimizing fraud and protecting their information, but they often lack the understanding and tools to do so.

- Financial institutions and retailers should continue to educate consumers on ways to protect their personal information and ways the firm protects the customers' information. This can enhance brand reputation and customer loyalty.
- Online merchants, in particular, can highlight security measures in place, such as Verified by Visa and Mastercard SecureCode, to feature security measures—even though there are many less-visible security measures also in place.
- Firms should include clear communication in FAQs and disclosures about the protections the organization has in place to protect consumer data. These protections should be in line with regulatory requirements and, when appropriate, should exceed such requirements.
- Consumers clearly view mobile-based communication, whether voice or SMS, as their preferred means of fraud notification. Organizations should pursue a range of mobile-based alert and communication options based on local preferences (i.e., voice, SMS, app push, and even others such as WhatsApp).
- Consumers are particularly concerned with fraud perpetrated through computer hacking. Firms can help alleviate these concerns through education and, in some cases, by offering tools such as anti-virus and anti-malware software to help mitigate these risks.

There is variability within geographies, which is often attributable to factors such as consumer buying habits, access to technology, prevalence of various payments products, and sociocultural norms. Some of these factors are in flux with changing technologies and demographics but highlight the fact that there is no “one size fits all” approach to engaging consumers in fraud management and securing their trust in and continued business with an organization.

RELATED AITE GROUP RESEARCH

Global Security Engagement Scorecard™, November 2016.

Digital Wallets: Provider Strategies to Meet Customer Requirements, September 2016.

2016 Global Consumer Card Fraud: Where Card Fraud Is Coming From, July 2016.

Digital-Channel Fraud Mitigation: The Mobile Force Awakens, June 2015.

Mobile Proximity Payments: A Disruption in the Force, May 2015.

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

Shirley Inscoe

+1.617.398.5050

sinscoe@aitegroup.com

Research Design and Data:**Judy Fishman**

+1.617.338.6067

jfishman@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