The Path to Digital Transformation

Controlling Friction While Tackling Cybercrime in Financial Services

May 2016

Sponsored by:

ThreatMetrix®
# Table of Contents

1. Executive Summary ............................................................................................................. 1  
   Study Findings.................................................................................................................. 1  
   Implications...................................................................................................................... 3  

2. The Digital Security Imperative .......................................................................................... 4  
   Increasing Digital Engagement ....................................................................................... 4  
   Importance of Digital Security ....................................................................................... 6  
   Keepers of the Keys .......................................................................................................... 7  

3. The True Casualty of Fraud ............................................................................................... 9  
   Banking & Payments Fraud Experience ....................................................................... 9  
   Effect of Banking & Payments Fraud ......................................................................... 11  

4. The Unseen Cost of Friction & Failure ............................................................................. 15  
   Step-Up Experience......................................................................................................... 15  
   Consumer Perceptions of Step-Up ............................................................................. 17  
   Consequences of Friction & Failure ............................................................................ 20  

5. Conclusion ......................................................................................................................... 23  
   Quantifying Lost Consumer Relationship Value ......................................................... 23  
   Recommended Actions ................................................................................................. 24  

6. Appendix: Study Objectives & Methodology..................................................................... 25
Table of Figures

Figure 2.1: Consumers’ Digital Behavior .................................................................................................................. 4
Figure 2.2: Frequency of Digital Banking Interactions & Purchase Transactions .......................................................... 5
Figure 2.3: Consumers’ Primary Security Concerns .................................................................................................. 6
Figure 2.4: Perceptions of Relative Security/Safety .................................................................................................... 7
Figure 3.1: Consumer Fraud Experience .................................................................................................................. 9
Figure 3.2: Information Compromised ..................................................................................................................... 10
Figure 3.3: Points of Fraud ......................................................................................................................................... 11
Figure 3.4: Attrition due to Fraud ............................................................................................................................ 12
Figure 3.5: Actions Taken to Secure/Re-Establish Accounts .................................................................................... 13
Figure 3.6: Average Annual Revenue per U.S. Checking Account (Illustrative) .......................................................... 14
Figure 4.1: Step-Up Experience .................................................................................................................................. 16
Figure 4.2: Step-Up Frequency .................................................................................................................................... 17
Figure 4.3: Perception of Step-Up ............................................................................................................................ 17
Figure 4.4: Account Lock-Out Experience and Frequency ......................................................................................... 18
Figure 4.5: Frustration with Account Lock-Out .......................................................................................................... 19
Figure 4.6: Perception of Step-Up by Account Lock-Out Frequency ........................................................................... 19
Figure 4.7: Service Disruptions While Traveling ...................................................................................................... 20
Figure 4.8: Impact of Step-Up on Consumer Behavior (Positive Perception) .............................................................. 21
Figure 4.9: Impact of Step-Up on Consumer Behavior (Negative Perception) .............................................................. 22
Figure 6.1: Survey Outline .......................................................................................................................................... 25
Figure 6.2: U.S. Respondent Demographics ............................................................................................................. 26
Figure 6.3: U.S. Respondents Regional Distribution .................................................................................................. 27
Figure 6.4: U.K. Respondent Demographics ............................................................................................................. 27
Figure 6.5: U.K. Respondents Regional Distribution .................................................................................................. 28
Figure 6.6: Australian Respondent Demographics .................................................................................................... 29
Figure 6.7: Australian Respondents Regional Distribution ........................................................................................ 29
Figure 6.8: Financial Product Ownership .................................................................................................................. 30
Figure 6.9: Respondent Distribution by Geographic & Demographic Segments ......................................................... 31
Figure 6.10: Respondent Distribution by Online Engagement Segment ..................................................................... 31
Figure 6.11: Online Engagement by Age .................................................................................................................. 32
About the Study Contributors

ThreatMetrix®, The Digital Identity Company, is the market-leading cloud solution for authenticating digital personas and transactions on the Internet. Verifying billions of annual transactions supporting tens of thousands of websites and thousands of customers globally through the ThreatMetrix® Digital Identity Network, ThreatMetrix secures businesses and end users against account takeover, payment fraud and fraudulent account registrations resulting from malware and data breaches. Key benefits include an improved customer experience, reduced friction, revenue gain, and lower fraud and operational costs. The ThreatMetrix solution is deployed across a variety of industries, including financial services, e-commerce, payments and lending, media, government, and insurance.

For more information about this study or related topics please contact us directly:

Armen Najarian  
Chief Marketing Officer  
+1 650 504 3430  
anajarian@threatmetrix.com  
@armennajarian

Alisdair Faulkner  
Chief Products Officer  
+1 650 796 5466  
afaulkner@threatmetrix.com

Vanita Pandey  
Vice President, Product Marketing  
+1 650 445 8854  
vpandey@threatmetrix.com  
@vanitatewari

Vince Lau  
Sr. Product Marketing Manager  
+1 408 200 5748  
vlau@threatmetrix.com
About the Study Contributors

First Annapolis is a specialized management consulting and mergers and acquisitions advisory firm with an unmatched focus on the payments industry. Founded in 1991, we advise clients on strategic and tactical matters across all major payment products and services including credit cards, debit cards, deposit access products, prepaid, and mobile payments.

For more information about this study or related topics please contact us directly:

**Josh Gilbert**  
*Partner, Payment Strategy & Innovation*  
+1 410 855 8515  
joshua.gilbert@firstannapolis.com

**Melissa Fox**  
*Manager, Payment Strategy & Innovation*  
+1 410 855 8518  
melissa.fox@firstannapolis.com
1. Executive Summary

There is no doubt we live in an increasingly digital world. We are in the midst of a digital transformation, as more and more consumers rely on online and—increasingly—mobile channels to conduct their everyday business. From banking to shopping to making plans with friends, digital interactions are becoming the primary mode of engagement for consumers of all ages.

This digital transformation is creating opportunities for banks to lower their service costs and provide increased convenience. But it is also creating inroads for fraudsters looking to leverage technology to steal debit/credit card data, gain access to consumer bank accounts, and/or open fraudulent accounts using a stolen identity. Digital account security has become an imperative for banks, retailers, and other providers, and it will only become more important over time.

The challenge banks face is preventing fraud and cybercrime while maintaining the quality of their digital experience. As consumers become more digitally engaged, their expectations increase. With access to unprecedented amounts of information, consumers demand more, better, and faster experiences. Nimble startups and innovative FinTech companies are threatening to erode bank margins, targeting consumers with a variety of alternatives to traditional banking products and services, and leveraging new technology to deliver lower cost services and potentially superior experiences. In this environment, banks must find ways to provide a streamlined, dynamic, and engaging experience, while at the same time maintaining the stalwart security and trust that is the cornerstone of traditional banking relationships.

Study results from multi-market research conducted in Q1 2016 suggest that banks need to invest not only in preventing fraud and cybercrime, but also in preventing the friction and failures that accompany consumer-facing prevention techniques in the digital environment. The penalty for failure is not just higher fraud losses and increased operating expenses, but loss of customer relationships: one year’s worth of fraud and friction is estimated to cost U.S. banks alone $14.9 billion in lost relationship value.

Study Findings

ThreatMetrix and First Annapolis partnered in early 2016 to conduct an industry-first study exploring consumer perceptions of online/mobile banking and payments security, with the intent of better understanding the effects of fraud and current digital security measures on consumers’ banking relationships.

Based on responses from 3,090 consumers evenly split across the U.S., U.K., and Australia, this multi-market study found that:

1. Consumers are highly engaged across digital channels for managing financial services.
   - 83% have accessed their bank account online in the past year, and 54% have downloaded and logged into the bank’s mobile app.
   - 70% of respondents reported logging into their bank’s online banking portal or mobile app at least once a week, while 29% said they log in daily.
   - Not surprisingly, these figures are even higher for younger consumers.

2. Security is an important concern for consumers, and perceptions of online/mobile security directly impact consumer brand trust and advocacy:
81% of consumers agreed with the statement “a bank's reputation for security is an important consideration when choosing a bank”.

62% agreed that they “would not recommend a bank to a friend” if they experienced fraud on their account.

In-store purchases are generally viewed as more secure than online and particularly mobile purchases, and online banking is generally viewed as more secure than mobile banking.

3. Banking and payments fraud is common—and the cost to financial institutions is not just hard-dollar losses and operational expenses, but lost consumer confidence and brand loyalty value as well.

38% of respondents reported having been a victim of banking/payments fraud.

Of that 38%, 10% left their financial institution all or in part as a result of having experienced fraud, taking with them all of their future revenue, cross-sell potential, and referral value.

Of those that remained with their financial institution, 90% took actions to secure/re-establish their accounts—most of which increase banks’ expenses.

Even after securing or re-establishing their account, consumers who have experienced fraud are likely to change their behavior in ways that lower banks’ revenues.

4. The cost of fraud prevention is significant, and so is the cost of friction created by well-intended, but often unnecessary step-up challenges. These measures directly impact customer loyalty and lifetime value.

83% of online/mobile banking users have experienced step-up challenges while logging in to their account in the past year, and 49% said step-up happens ‘always’ or ‘frequently’.

Of that 83%, 68% said that being asked to perform additional steps during online account log-in has a positive effect on their feelings about their bank, and 22% view it as neutral.

For 10%, however, the experience has a negative impact on how they view their interaction: it is cumbersome, annoying, and for some, a serious inconvenience.

Of those who said that being asked to perform additional steps had a ‘negative’ effect on their perception of their banking interaction, 76% said it affected their behavior:

- 30% changed banks (and another 32% considered changing banks);
- 26% called customer service to complain;
- A net 26% used online/mobile banking less often; and
- A net 9% said they use the payment linked to the account less often.

Highly-engaged digital consumers are most likely to perceive step-up as a negative, and to change their behavior as a result of being stepped up:

- 17% of heavy online/mobile users reported step-up having a negative impact on their feelings about their banking interaction.
- 52% of heavy online/mobile users said it affected their behavior—and 18% of those said they changed banks as a result.

Overall, 3% of respondents who experienced step-up during their online/mobile account login said that they closed an account/changed banks as a result.
Implications

Fraud and security-related friction are costly for banks in many ways: in addition to fraud losses and operating costs, there’s the lost revenue and profitability from the attrition and dilution of account relationships and brand advocacy. As we continue to undergo a digital transformation, security will only become more important, and the likelihood of a negative experience due to friction and failure will only increase—as will the downside risks for financial institutions.

While there are many costly implications of account re-establishment and potential consumer behavior changes, the risk of incremental attrition is the most detrimental to banks.

Consider the illustrative application of the study findings for U.S. financial institutions as an example:

- Based on the study results, we estimate that one year’s worth of fraud victims represents $4.9 billion in lost future relationship value above and beyond U.S. banks’ fraud losses and operational expenses.

- Study results also suggest that U.S. banks lose an additional $10.0 billion in relationship value from customer attrition due to the friction created by current step-up practices.

Together, that’s $14.9 billion in lost relationship value for one year’s activity. Assuming consistent levels of fraud and friction over a five-year period (likely a best-case scenario given current trends), that lost relationship value becomes $74.3 billion. The actual opportunity cost of that attrition—factoring the lost value of referrals, future cross-sell opportunities, etc.—would be even higher.

These losses become cumulative and ongoing, until changes are made to prevent the fraud and friction that is compelling consumers to seek an alternative.

* * *

As we continue to undergo this digital transformation, having a robust digital security strategy that focuses on both preventing cybercrime and preserving the digital experience is key. Cybercriminals will continue to invest in their fraud strategies, and banks need to make the same investment in proactive cybersecurity prevention. Avoiding both fraud and friction is important today—and will only become more so in the future.
2. The Digital Security Imperative

There is no denying that we live in a digital world. We are in the midst of a digital transformation, as consumers of all walks of life now shop, bank, and socialize online and, increasingly, via mobile devices. Digital interactions permeate every aspect of our daily lives, influencing the decisions we make, the way we transact, and the way we engage with others. Protecting consumers’ personal information in a digital world has become an imperative for banks, retailers, and other providers, and it will only become more important over time.

To this end, ThreatMetrix and First Annapolis partnered to explore consumer perceptions of online/mobile banking and payments security. The intent is to better understand the effects of fraud and current preventative measures on consumers’ banking relationships. Study results are based on a sample of 3,090 consumers from the U.S., U.K., and Australia. For details about the study objectives and methodology, including sample demographics and segment definitions, please see the Appendix.

Increasing Digital Engagement

Consumers are highly engaged across both online and mobile channels for managing financial services:

- **90%** of respondents report having made a purchase online in the past year, and **51%** have made a purchase using their mobile device.
- **83%** have accessed their bank account online, and **54%** have logged in via a mobile app.
- **63%** have used online or mobile bill pay.

*Figure 2.1: Consumers’ Digital Behavior*

“Please indicate which of the following you have done within the last year.”

Adoption levels are consistently high across all three markets. But while online usage levels are consistent across age segments, use of mobile devices is most prevalent among younger consumers,
portending future macro-shifts in consumer behavior and underscoring the importance of digital channels in all forms. This shift is particularly important when considering that younger consumers will account for nearly 100% of new-to-bank account openings in the coming years, and for many of them, their preferred engagement model is digital-first.

Shopping and banking are common everyday activities, and the frequency with which those interactions are taking place in the digital environment is rapidly accelerating. For many consumers, shopping and banking online or via their mobile device are daily activities:

- 70% of respondents reported logging into their bank’s online banking portal or mobile app at least once a week, while 29% said they log in daily.
- 36% of respondents say they make a purchase online or using their mobile device at least once a week, while 7% are daily shoppers.

**Figure 2.2: Frequency of Digital Banking Interactions & Purchase Transactions**

<table>
<thead>
<tr>
<th>Online/Mobile Banking</th>
<th>Online/Mobile Shopping</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Over the period of a month, how frequently (on average) do you log into your bank’s online banking portal or mobile app?”</td>
<td>“Over the period of a month, how often (on average) do you make purchases online or using your mobile device?”</td>
</tr>
</tbody>
</table>

This is good news for banks, which have a vested interest in encouraging consumers to interact via their online and mobile channels. Digital channels are a win-win for banks in that they can lower the cost of service while driving increased engagement. Digital interactions have a significantly lower cost-to-serve than branch or call center interactions, and consumers who are frequent online/mobile banking users tend to be active and highly engaged, which is a good indicator of favorable retention rates and revenue potential. Across the boards, banks have an opportunity to better engage consumers of all ages through their digital channels.
Importance of Digital Security

With digital channels becoming increasingly important venues for banking and commerce, digital security is of paramount importance: cybercrime costs consumers, ecommerce merchants, and financial institutions an estimated $274 billion per year globally.\(^1\)

And security is an important concern for consumers:

- **55%** of respondents agreed (and **17%** strongly agreed) with the statement “I am extremely concerned about the risk of banking and payments-related fraud.”
- **46%** said their level of concern has increased in the past two years.
- **65%** said they feel “extremely anxious” when they hear a data breach might have affected them.

Consumers are most concerned that their personal information will be compromised and used to steal their identity. Their second greatest concern is that their bank account information will be compromised, followed by their debit/credit card information being compromised.

**Figure 2.3: Consumers’ Primary Security Concerns**

*“Which of the following security risks are you most concerned about?”*

![Chart showing consumers' primary security concerns](chart)

Note: “Other” includes general fraud, EMV chip loss, and unauthorized computer access.

Consumers perceive the relative security of transactions across various channels and payment methods differently. In-store purchases are generally viewed as more secure than online and, in particular, mobile purchases, and online banking is generally viewed as more secure than mobile banking. Many consumers, particularly older consumers, are skeptical of storing payment card information with an online retailer/wallet provider and using mobile payments for in-store purchases (i.e., using Apple Pay, Android Pay, Samsung Pay, etc.).

---

\(^1\) ThreatMetrix, "Combating Cybercrime - A Collective Global Response", 2013
Younger consumers tend to view digital channels as more secure—but the perceived gap between physical and digital channel security remains.

If banks and retailers are going to close the gap between perceptions of physical vs. digital security, building consumer confidence—without hindering the digital experience—will be critical.

**Keepers of the Keys**

Consumers view both banks and online retailers/wallet providers as responsible for safeguarding their digital identities and payment information, but they are more likely to hold their bank accountable:

- **72%** of respondents agreed (including **30%** who strongly agreed) with the statement “my bank is responsible for monitoring activity on my account and preventing potentially fraudulent transactions.” (7% disagreed).
- **54%** of consumers agreed with the statement “online retailers/wallet providers are responsible for monitoring activity and preventing potentially fraudulent transactions.” (13% disagreed).

For most consumers, security is an important factor when selecting and recommending a bank:

- **81%** of consumers agreed (including **47%** who strongly agreed) with the statement “a bank’s reputation for security is an important consideration when choosing a bank”. (4% disagreed).
- **62%** agreed that they would not recommend a bank to a friend if they experienced fraud on their account. (11% disagreed).

These are important data points because referrals from friends and family are the **#1 reason** consumers cite when asked why they chose their primary bank.² And while the attitudes above are generally

---

consistent across age segments, they become even more important when thinking about younger consumers, who tend to rely more heavily on social media and word-of-mouth than those before them.

As digital channels become the primary means of engagement for many consumers, banks (and online retailers and wallet providers as well) are faced with the critical challenge of protecting themselves and consumers from digital security attacks—without compromising the digital experience.
3. The True Casualty of Fraud

Fraud events cost financial institutions billions of dollars per year in the form of hard-dollar losses and operational expenses—not including the collateral cost of brand reputation damage, account attrition, and value dilution of compromised accounts.

Banking & Payments Fraud Experience

Banking and payments fraud\(^3\) is not uncommon: 38% of respondents reported having been a victim of banking/payments fraud (18% in the last two years, and 20% three or more years ago).

These findings are fairly consistent across markets, although precise figures vary, with respondents in the U.S. more likely to indicate recent fraud experience than those in the U.K. or Australia.

**Figure 3.1: Consumer Fraud Experience**

“Have you ever been a victim of banking/payments fraud?”

Payment card information is the most vulnerable, with 66% of respondents who experienced fraud in the last two years reporting that their credit or debit card information was compromised.

---

\(^3\) Banking or payments fraud was defined in the survey as “when another person obtains your bank account information, debit/credit card number, or other personal information and uses it to make purchases or withdraw money from your account without your consent.”
When consumers’ personal or payment information is compromised, fraudsters often leverage online and mobile channels to perpetrate fraud:

- **45%** indicated that their compromised information was used to make online or mobile purchases.
- **43%** indicated that it was used to make in-store purchases.
- **12%** reported that it was used to transfer funds out of their bank account.
Figure 3.3: Points of Fraud
“How was the compromised information used?”

<table>
<thead>
<tr>
<th></th>
<th>U.S.</th>
<th>U.K.</th>
<th>AU</th>
</tr>
</thead>
<tbody>
<tr>
<td>To make online/ mobile purchases</td>
<td>45%</td>
<td>51%</td>
<td>40%</td>
</tr>
<tr>
<td>To make purchases in stores</td>
<td>43%</td>
<td>41%</td>
<td>34%</td>
</tr>
<tr>
<td>To transfer funds out of my bank account</td>
<td>12%</td>
<td>14%</td>
<td>17%</td>
</tr>
<tr>
<td>To open a new account(s) in my name</td>
<td>10%</td>
<td>13%</td>
<td>5%</td>
</tr>
<tr>
<td>To withdraw cash at an ATM</td>
<td>8%</td>
<td>7%</td>
<td>8%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
<td>3%</td>
<td>5%</td>
</tr>
</tbody>
</table>

Note: “Other” includes overseas transactions, airline ticket purchases, etc.

Only in the U.S. did a higher percentage of consumers report that their compromised information was used in stores versus digital channels. U.S. respondents are also most likely to report that it was their credit or debit card information that was compromised and used to perpetuate fraud (see Figure 3.2).

Both of these likely reflect the difference in EMV migration across the three markets. Chip cards are more difficult to counterfeit than traditional mag-stripe cards and often have additional security features (e.g., PIN requirements) that make it more difficult to use stolen cards or card information at the physical point of sale. In the U.K. and Australia, this avenue has already been closed to fraudsters—but for U.S. banks and retailers, the shift to EMV is still underway. The shift from card-present to card-not-present fraud in markets with EMV is well-documented, and we anticipate a near-term shift in U.S. fraud dynamics that will only heighten the importance of digital security.

**Effect of Banking & Payments Fraud**

As noted above, fraud events have direct financial implications for banks: there are hard-dollar losses and significant operational costs associated with remediation. Similarly for consumers, there are costs in the form of hard-dollar losses and time spent resolving fraud-related issues:

- **19%** of respondents who experienced fraud in the last two years indicated that they lost money as a result, with reported median losses of $155.
- **38%** of respondents with recent fraud experience indicated that resolution required less than an hour of active time—but **10%** reported that it required 7 hours or more.

There is no doubt that a fraud event is a negative experience—and for many consumers, the experience translates into actions (attrition, account re-establishment, and behavior changes) that have significant cost implications for their financial institutions.
Increased Attrition

Among the 38% of respondents who have experienced a fraud event, 10% left their financial institution all or in part as a result of having experienced fraud.

This suggests that when a consumer experiences fraud there is a 1 in 10 chance that they attrite—and take all of their future revenue and cross-sell potential with them. With average expected revenue of $5,090 in the U.S. over the life of a relationship, that incremental attrition is costly for banks:

- Younger respondents who have experienced fraud are most likely to have left their financial institution as a result of their fraud experience: 18% of fraud victims under 35 reported leaving their bank at least partly due to the fraud/compromise.
- U.S fraud victims were also more likely to have left as a result of their fraud/compromise experience (14%). With thousands of financial institutions to choose from, perceptions of security are an important competitive factor.

Figure 3.4: Attrition due to Fraud

% of respondents that experienced a recent or historical fraud event and indicated that the fraud event was the reason/one of the reasons for their departure

---

\[4\] Assumes $760 average annual relationship revenue and 6.7-year average length of relationship
**Consumer Burden & Increased Expense**

Consumers that leave their bank bear the burden of opening a new account elsewhere—switching direct deposits or automatic payments, setting up online banking/bill pay, ordering new debit cards or checks, all of which are a hassle. For those consumers who remain with their bank, they must go through many of the same obstacles—and the bank must incur many of those same costs, without the benefit of new relationship acquisition.

Of those who have experienced fraud in the past two years and are still with their bank:

- **71%** were reissued a new debit card and **30%** changed their PIN.
- **27%** changed their login/password.
- **13%** closed the compromised account.

Only **10%** did not take any actions as a result of the fraud.

**Figure 3.5: Actions Taken to Secure/Re-Establish Accounts**

“What actions did you take as a result of the fraud incident/compromise?”

<table>
<thead>
<tr>
<th>Action</th>
<th>U.S.</th>
<th>U.K.</th>
<th>AU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received a new debit/credit card</td>
<td>80%</td>
<td>63%</td>
<td>66%</td>
</tr>
<tr>
<td>Changed my PIN</td>
<td>27%</td>
<td>28%</td>
<td>35%</td>
</tr>
<tr>
<td>Changed my login/password</td>
<td>26%</td>
<td>26%</td>
<td>28%</td>
</tr>
<tr>
<td>Closed my account (but stayed with the same bank)</td>
<td>17%</td>
<td>9%</td>
<td>11%</td>
</tr>
<tr>
<td>Changed/updated my online bill payment settings</td>
<td>10%</td>
<td>6%</td>
<td>7%</td>
</tr>
<tr>
<td>Changed/updated my automatic payment settings</td>
<td>10%</td>
<td>5%</td>
<td>6%</td>
</tr>
<tr>
<td>Changed/updated my direct deposit settings</td>
<td>6%</td>
<td>0%</td>
<td>7%</td>
</tr>
<tr>
<td>Reordered checks</td>
<td>5%</td>
<td>6%</td>
<td>2%</td>
</tr>
<tr>
<td>Signed up for credit monitoring service</td>
<td>6%</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>None of the above</td>
<td>6%</td>
<td>13%</td>
<td>13%</td>
</tr>
</tbody>
</table>

Some of these actions, like card reissuance, have direct hard dollar costs; others may have soft dollar costs in the form of increased service costs or increased friction when consumers forget their new PINs or passwords. Even if there is no change in consumer behavior, these actions erode the profitability of the relationship.
Consumer Behavior Changes & Decreased Revenue

After securing or re-establishing their account, consumers who have experienced fraud are likely to change their behavior in response to the fraud/compromise—and those changes can be costly:

- **34%** (44% of those under 35) indicated that they **make fewer purchases** as a result of their fraud experience.
- **A net 5%** reported using their debit/card less.\(^5\)
- **A net 4%** reported using cash or checks more.\(^6\)

Every transaction not made—or made using a different payment method (e.g., cash, check, another bank’s card)—represents a lost revenue opportunity. And while revenue on individual transactions is measured in pennies, the aggregate impact on account economics is significant: First Annapolis estimates that a highly active debit account generates, on average, 40-45% more revenue than a moderately active account—which in turn generates 25-30% more revenue than an account with light activity.

**Figure 3.6: Average Annual Revenue per U.S. Checking Account (Illustrative)**

Source: First Annapolis Consulting

While the bank may have retained the account and the relationship, to the extent that account activity declines in the wake of a fraud event, the decrease in revenue from the relationship can still be significant. And for younger consumers who are still developing their banking and payments habits, the experience can be particularly damaging as far as their long-term behavior and revenue potential.

When fraud occurs, the true cost for banks (and often retailers as well) is not just the dollars stolen and the operational expenses required, but the relationships lost and profitability diminished.

---

\(^5\) 12% report using their debit/credit card less, while 7% report using a debit/credit card more

\(^6\) 11% report using cash/checks more, while 7% report using them less
4. The Unseen Cost of Friction & Failure

Given the heavy costs associated with fraud, prevention is—and should be—a top priority for banks. The challenge is that 95%-98%\(^7\) of the time, the person attempting to access an account or make a purchase is a legitimate consumer. But in the effort to detect the 2%-5% of times a fraudster is trying to access the account, banks and retailers make consumers jump through hoops to prove they are who they say they are—and that creates its own set of costs and downside effects.

As with actual fraud, introducing friction into the digital experience has the potential to dilute the quality and economics of banks’ relationships—and potentially puts a bank at risk of losing relationships altogether. This is especially true of highly active users with lucrative account economics and younger consumers with significant long-term revenue potential (and high expectations for their digital interactions).

**Step-Up Experience**

To stem the rise of cybercrime, many banks and ecommerce merchants have implemented additional digital security challenges—often referred to as ‘step-up challenges’—designed to ferret out fraudsters using malware, Trojans, spyware, keyloggers or bot networks and prevent them from opening/accessing accounts and perpetrating fraudulent transactions. These step-up challenges may include requiring consumers to answer additional questions, enter a code sent via text or email, or input a CAPTCHA value, and they all have one thing in common: they put the burden of authentication back on the consumer. They also create a potential point of failure in an interaction or transaction—even for legitimate consumers.

Respondents are no strangers to step-up challenges: 83% of online/mobile users have experienced step-up challenges while logging in to their account in the past year, and 68% reported having been stepped up while making an online purchase. U.S. respondents are more likely than those from the U.K. or Australia to have experienced step-up, as are younger consumers and heavily engaged online/mobile users.

---

\(^7\) ThreatMetrix, "Combating Cybercrime - A Collective Global Response", 2013
Figure 4.1: Step-Up Experience

Online/Mobile Banking
“Which of the following have you been required to do when attempting to log in to your bank’s website online or via your mobile device?”

Online/Mobile Shopping
“Which of the following have you been required to do when making a purchase online or via your mobile device?”

% of respondents that have experienced step-up challenges by segment

<table>
<thead>
<tr>
<th>Market</th>
<th>U.S.</th>
<th>U.K.</th>
<th>AU</th>
<th>Under 35</th>
<th>35 to 54</th>
<th>55 and Over</th>
<th>Online Engagement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking</td>
<td>91%</td>
<td>84%</td>
<td>75%</td>
<td>89%</td>
<td>82%</td>
<td>78%</td>
<td>Heavy</td>
</tr>
<tr>
<td>Shopping</td>
<td>65%</td>
<td>70%</td>
<td>69%</td>
<td>75%</td>
<td>69%</td>
<td>61%</td>
<td>Light</td>
</tr>
</tbody>
</table>

*Options included: answer additional security questions [selected by 78% for banking and 44% for shopping]; enter a code sent to me via text/email [60% / 44%]; re-enter my user name/password or card number/PIN [49% / 32%]; enter a CAPTCHA value (e.g., type in distorted text or select a particular image/set of images to provide you are human) [32% / 47%]; and other [4% / 2%] (responses included biometric authentication and recognition of pre-selected image)

For many respondents, particularly those who are younger, step-up challenges are a frequent occurrence. Of those who have experienced step-up challenges:

- **49%** said step-up happens ‘always’ or ‘frequently’ when logging in to online/mobile banking.
- **58%** of those under 35 said that they experience step-up challenges ‘always’ or ‘frequently’, compared to **42%** of those 55 and over.
Consumer Perceptions of Step-Up

Consumers’ conscious perceptions of step-up in their banking and ecommerce interactions are generally positive. When asked, 68% of respondents said that being asked to perform additional steps during online/mobile account log-in has a positive effect on their feelings about their bank, and 22% view it as neutral. For 10% of respondents, however, the experience has a negative impact on how they view their interaction: it is cumbersome, annoying, and for some, a serious inconvenience.

Being stepped-up during an ecommerce transaction has a similar impact on consumers’ perceptions of their interaction: most consumers view it neutrally or positively, but 11% view it negatively.

Figure 4.3: Perception of Step-Up

“How does being asked to perform additional steps affect your feelings about your interaction with your bank [the online retailer/wallet providers]?”

- Extremely positively—they’re preventing fraud on my account
- Somewhat positively—it makes me feel more secure, even if it is a bit inconvenient
- Neither positively nor negatively
- Somewhat negatively—it’s cumbersome and annoying, even if they are attempting to prevent fraud
- Extremely negatively—it’s a serious inconvenience and they need to find a better way
Highly-engaged digital consumers are most likely to perceive step-up as a negative:

- 17% of heavy online/mobile users report that being stepped up has a negative effect on their perceptions of their online/mobile banking interaction, compared to 8% of moderate users and 6% of light users.
- 20% of respondents who are heavy online/mobile users report a negative effect on their perceptions of their ecommerce interaction, compared to 9% of moderate users and 6% of light users.

Step-up challenges increase friction: they require additional information, add time, and often delay consumers from completing their interactions. In most cases consumers pause, pass the additional step-up challenges, and continue with their interaction. But many times legitimate consumers fail the challenges or mis-key their password too many times, and they find themselves (at least temporarily) locked out of their account.

Account lock-out is a common experience:

- 53% of online/mobile banking users report having been ‘locked out’ of their account at some point.
- Of those, 8% say that they are locked out ‘often’, and 28% say that they are locked out ‘occasionally’.

**Figure 4.4: Account Lock-Out Experience and Frequency**

“Have you ever been ‘locked out’ of online/mobile banking for failing to enter the correct user name/password and/or pass additional screening questions?”
At this point, friction becomes a point of failure and consumers are prevented from conducting their interaction—which most find highly frustrating. When those who have experienced lock-out were asked to rate their frustration on a scale from 0 (Not at all Frustrating) to 10 (Extremely Frustrating), **1 out of 5 rated it a ‘10’, while more than 50% rated it a ‘7’ or higher.**

![Figure 4.5: Frustration with Account Lock-Out](image)

“How frustrating do you find it when you are ‘locked out’ online/mobile banking?”

Consumers’ experience with account lock-out appears to have an effect on how they feel about the step-up process and the impact it has on their banking interaction: only **1 out of 25 people** who have never been locked out say that being stepped up has a negative effect on their interaction, compared to nearly **1 out of 3 people** who say it happens often.

![Figure 4.6: Perception of Step-Up by Account Lock-Out Frequency](image)

We observe a similar phenomenon when consumers are traveling:

- **31%** of travelers have experienced a service disruption while on the road (and of those, **11%** experience disruptions frequently).
- **33%** of those affected say it has a negative impact on their feelings about their bank.
**Figure 4.7: Service Disruptions While Traveling**

**Frequency of Disruptions**

“While traveling, have you ever experienced a service disruption (i.e., been unable to log into your bank account or use your card until you have contacted your bank)?”

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Yes, frequently</th>
<th>Yes, occasionally</th>
<th>No, because I provide notice to my bank in advance</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage</td>
<td>3%</td>
<td>28%</td>
<td>19%</td>
<td>50%</td>
</tr>
</tbody>
</table>

**Perception of Experience**

“How do you feel about being contacted by your bank (or having to contact your bank) while traveling?”

- **Frequently**
  - Positive: 33%
  - Neutral: 16%
  - Negative: 51%

- **Occasionally**
  - Positive: 44%
  - Neutral: 23%
  - Negative: 31%

---

**Consequences of Friction & Failure**

Unfortunately for banks, a positive perception of step-up challenges appears to do little to influence consumer behavior in ways that are positive for the bank: it is unlikely to increase engagement, drive incremental transactions, or improve retention. The best case scenario, in most cases, is that it results in no change in behavior.

Even those who have a positive perception of step-up can have a negative reaction to the experience. Among respondents who said that being asked to perform additional steps had a positive effect on their perception of their banking interaction, 74% said that it had no effect on their behavior. Of the 26% who said it affected their behavior:

- **40%** called customer service to complain.
- **A net 12%** said they use online/mobile banking **less often** as a result.\(^8\)
- **13%** said that they considered closing their account/changing banks; another **7%** actually did.

---

\(^8\) 20% said they use it more often; 32% said they use it less often
In most cases, a positive perception does not result in behavior changes—but the same cannot be said of a negative one. When legitimate consumers experience friction or fail step-up challenges and perceive their banking interactions negatively, those perceptions are much more likely to manifest in behavior changes that negatively affect their bank.

Of those who said that being asked to perform additional steps had a ‘negative’ effect on their perception of their banking interaction, only 24% said that it had no effect on their behavior. Of the 76% who said it affected their behavior:

- 30% changed banks (and another 32% considered changing banks).
- 26% called customer service to complain.
- A net 26% used online/mobile banking less often.
- A net 9% said they use the payment linked to the account (e.g., debit or credit card) less often.
Overall, 3% of respondents who experienced step-up during their online/mobile account login said that they closed an account/changed banks as a result.

The implications of friction and failure are profound for banks:

- Every consumer who leaves the bank takes with them the life-time value of their account; their future cross-sell potential; and their referrals to other potential new customers.
- Every time a consumer chooses a different payment method over their debit or credit card, their bank loses revenue.
- Every time a consumer calls to complain, or calls the contact center or visits a branch in lieu of logging in to online or mobile banking, their bank’s servicing costs increase.

These dynamics become even more important when you consider that the consumers most likely to have a negative view of step-up are those who the bank most wants to attract and retain: younger consumers and those who tend to be highly engaged. As we continue to undergo a digital transformation at the macro level, the likelihood of a negative experience due to friction and failure will only increase—as will the downside risks and financial impacts for financial institutions.
5. Conclusion

Fraud and security-related friction are costly for banks in many ways: in addition to fraud losses and operating expenses, there’s the lost revenue and profitability from the attrition and dilution of relationships.

**Quantifying Lost Consumer Relationship Value**

While there are many costly implications of account re-establishment and potential consumer behavior changes, the risk of incremental attrition is the most detrimental to banks. Consider the U.S. market as an example:

- There are an estimated 215.1 million banked consumers over 18 in the U.S.\(^9\)
- 9% of respondents experienced banking/payments fraud within the last 12 months; that translates into 19.4MM fraud victims in the U.S.
- 10% of respondents who experienced fraud left their bank as a result; that suggests banks lost 1.9MM relationships due to fraud.

This data implies that one year’s worth of fraud victims represents **$4.9 billion** in lost future relationship value\(^10\) above and beyond banks’ fraud losses and operational expenses.

One way for banks to prevent fraud and cybercrime and their downstream effects would be to batten down the hatches—implement stringent screening/challenge processes and positively verify a consumer’s identity every time they log in to their account or attempt to make a purchase. But that’s not a good idea:

- 74% of the 215.1 million banked consumers are active online banking users;\(^11\) that’s 157.7 million active online/mobile banking users\(^12\).
- Study results suggest that 83% of online/mobile banking users are likely to experience step-up challenges—and 3% of them are likely to leave their bank as a result.
- That suggests that banks could lose 3.9 million relationships due to friction.

That’s **$10.0 billion** in lost relationship value\(^13\) due to the friction and failures. Together with the relationships lost due to fraud, that’s **$14.9 billion** in lost relationship value. Assuming consistent levels of fraud and friction over a five-year period (likely a best-case scenario given current trends), that lost relationship value becomes **$74.3 billion**. The actual opportunity cost of that attrition—factoring the lost value of referrals, future cross-sell opportunities, etc.—would be even higher.

These losses become cumulative and ongoing, until changes are made to prevent the fraud and friction that is compelling consumers to seek an alternative.

---

9 US Census; Federal Reserve, Consumers and Mobile Financial Services 2015
10 Assumes $760 average annual relationship value, 6.7-year average length of relationship, and average 50% remaining at the time of the fraud
11 Federal Reserve, Consumers and Mobile Financial Services 2015
12 Excludes the estimated 1.9 million consumers who attrited due to fraud
13 Assumes $760 average annual relationship value, 6.7-year average length of relationship, and average 50% remaining at the time of attrition
Recommended Actions

Study results suggest that banks need to invest not only in preventing fraud and cybercrime, but also in preventing the friction and failures that accompany consumer-facing prevention techniques in the digital environment.

To this end, banks would benefit from:

- Taking a **holistic approach** to digital security that encompasses all of their digital channels and potential endpoints—PCs, tablets, mobile devices—and consider both **device profiles** and **user profiles** in evaluating potential fraud.
- Leveraging **real-time technology** and **network solutions** to be as **agile** as possible in identifying and responding to fraud trends and events.
- When evaluating digital security solutions, considering not only their ability to prevent fraud, but also **their impact on the customer experience**. Focus on preventing false positives and identifying legitimate consumers **without** creating friction and requiring their active participation.
- Involving a **cross-functional group of stakeholders** in developing their digital security strategy; preventing fraud and friction is **not the sole responsibility** of the security unit or IT group.
- Evaluating/re-evaluating fraud policies on an **ongoing basis**: establish a baseline; monitor results and feedback; and incorporate those learnings into their fraud strategies over time.

As we undergo this digital transformation, having a robust digital security strategy that focuses on both preventing cybercrime and preserving the digital experience is key. Cybercriminals will continue to invest in their fraud strategies, and banks need to make the same investment in proactive cybercrime prevention. **Avoiding both fraud and friction** is important today—and will only become more so in the future.
6. Appendix: Study Objectives & Methodology

This study explores consumer perceptions of security as it relates to online/mobile banking and payments. It was designed to address the following questions:

- What are consumers’ attitudes toward digital security?
  - How important is the issue of digital security?
  - What are they most concerned about?
  - How do they perceive the relative security of different online banking and payment activities?
- How do consumers feel about going through additional security screenings, and what, if any, affect does it have on their behavior and relationship with a bank, retailer, or wallet provider?
- What affect does experiencing banking and payments fraud have on consumer behavior and their relationship with their financial institution?

Research Methodology

To answer these questions, First Annapolis and ThreatMetrix designed a multi-market consumer survey. Research Now, an online sampling and data collection company, administered the online survey to consumer panels in the U.S., U.K., and Australia in March 2016.

The survey had four parts, as outlined below; qualified consumers were asked to respond to 38 questions. The same survey was administered across all three markets, with minor adjustments to reflect the local language and cultural norms.

Figure 6.1: Survey Outline

<table>
<thead>
<tr>
<th>Survey Outline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background &amp; Screening Questions</td>
</tr>
<tr>
<td>- Consumer demographics (age, zip/post code, gender, income, ethnicity, employment)</td>
</tr>
<tr>
<td>- Product ownership (devices, financial products)</td>
</tr>
<tr>
<td>Perceptions of Digital Security</td>
</tr>
<tr>
<td>- Online banking and shopping activity (adoption, frequency)</td>
</tr>
<tr>
<td>- Perceived security of online banking/payments activities</td>
</tr>
<tr>
<td>- Primary concerns</td>
</tr>
<tr>
<td>- Perception of responsibility for digital security and fraud prevention</td>
</tr>
<tr>
<td>Experience with Enhanced Digital Security</td>
</tr>
<tr>
<td>- Type/frequency of step-up activities during account log-in or travel</td>
</tr>
<tr>
<td>- Impact on consumer feelings regarding the interaction</td>
</tr>
<tr>
<td>- Effect on consumer behavior</td>
</tr>
<tr>
<td>Experience with Banking/Payments Fraud</td>
</tr>
<tr>
<td>- Type of compromise (data captured, fraud perpetrated)</td>
</tr>
<tr>
<td>- Consumer impact (cost, time to resolution)</td>
</tr>
<tr>
<td>- Effect on consumer behavior and banking relationship</td>
</tr>
</tbody>
</table>
Survey Sample

Findings are based on responses from 3,090 consumers from the U.S., U.K., and Australia. In general, survey responses were highly consistent across markets. Significant market-specific variations are highlighted throughout the report, but overall findings are based on the combined sample.

In order to qualify for the survey, consumers were required to be over 18 and to be ‘banked’, meaning they indicated ownership of a checking account (a “current account” in the U.K. or a “cheque account” in Australia) and/or debit card.

U.S. Sample

U.S. findings are based on a sample of 1,013 consumers. While not statistically representative of the U.S. population, the sample is sufficiently balanced to draw meaningful conclusions about consumer attitudes towards digital security.

Figure 6.2: U.S. Respondent Demographics

<table>
<thead>
<tr>
<th></th>
<th>Sample Count</th>
<th>% of Sample</th>
<th>% of U.S. Population</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total</strong></td>
<td>1,013</td>
<td>100.0%</td>
<td>--</td>
</tr>
<tr>
<td><strong>Gender</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>468</td>
<td>46.2%</td>
<td>49.2%</td>
</tr>
<tr>
<td>Female</td>
<td>545</td>
<td>53.8%</td>
<td>50.8%</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18-24</td>
<td>142</td>
<td>14.0%</td>
<td>13.0%</td>
</tr>
<tr>
<td>25-34</td>
<td>188</td>
<td>18.6%</td>
<td>17.6%</td>
</tr>
<tr>
<td>35-44</td>
<td>187</td>
<td>18.5%</td>
<td>16.9%</td>
</tr>
<tr>
<td>45-54</td>
<td>177</td>
<td>17.5%</td>
<td>18.4%</td>
</tr>
<tr>
<td>55-64</td>
<td>167</td>
<td>16.5%</td>
<td>16.1%</td>
</tr>
<tr>
<td>65+</td>
<td>152</td>
<td>15.0%</td>
<td>18.0%</td>
</tr>
<tr>
<td><strong>Household Income</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Less than $25,000</td>
<td>245</td>
<td>24.2%</td>
<td>23.2%</td>
</tr>
<tr>
<td>$25,000 to $49,999</td>
<td>284</td>
<td>28.0%</td>
<td>23.7%</td>
</tr>
<tr>
<td>$50,000 to $74,999</td>
<td>162</td>
<td>16.0%</td>
<td>17.8%</td>
</tr>
<tr>
<td>$75,000 to $99,999</td>
<td>136</td>
<td>13.4%</td>
<td>12.2%</td>
</tr>
<tr>
<td>$100,000 to $149,999</td>
<td>104</td>
<td>10.3%</td>
<td>13.0%</td>
</tr>
<tr>
<td>$150,000 to $199,999</td>
<td>36</td>
<td>3.6%</td>
<td>5.0%</td>
</tr>
<tr>
<td>$200,000 or more</td>
<td>35</td>
<td>3.5%</td>
<td>5.0%</td>
</tr>
<tr>
<td>Prefer not to answer</td>
<td>11</td>
<td>1.1%</td>
<td>--</td>
</tr>
<tr>
<td><strong>Ethnicity</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Native American, Inuit or Aleut</td>
<td>12</td>
<td>1.2%</td>
<td>0.8%</td>
</tr>
<tr>
<td>Asian American/Pacific Islander</td>
<td>54</td>
<td>5.3%</td>
<td>5.2%</td>
</tr>
<tr>
<td>African American/Black/Caribbean American</td>
<td>142</td>
<td>14.0%</td>
<td>12.6%</td>
</tr>
<tr>
<td>Caucasian/White</td>
<td>709</td>
<td>70.0%</td>
<td>73.8%</td>
</tr>
<tr>
<td>Other</td>
<td>88</td>
<td>8.7%</td>
<td>7.6%</td>
</tr>
<tr>
<td>Prefer not to answer</td>
<td>8</td>
<td>0.8%</td>
<td>--</td>
</tr>
<tr>
<td>Of Hispanic/Latin Descent</td>
<td>182</td>
<td>18.0%</td>
<td>16.9%</td>
</tr>
<tr>
<td>Not of Hispanic/Latin Descent</td>
<td>825</td>
<td>81.4%</td>
<td>83.1%</td>
</tr>
<tr>
<td>Prefer not to answer</td>
<td>6</td>
<td>0.6%</td>
<td>--</td>
</tr>
</tbody>
</table>

Source: U.S. Census Bureau, American Community Survey (2014)
Respondents represent 48 out of 50 states (no respondents from Vermont or Alaska), and distribution is broadly aligned with the U.S. population, as shown below.

*Figure 6.3: U.S. Respondents Regional Distribution*\(^\text{14}\)

<table>
<thead>
<tr>
<th>Population Distribution</th>
<th>Sample Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>West 24%</td>
<td>West 23%</td>
</tr>
<tr>
<td>Northeast 18%</td>
<td>Northeast 19%</td>
</tr>
<tr>
<td>Midwest 21%</td>
<td>Midwest 23%</td>
</tr>
<tr>
<td>South 37%</td>
<td>South 35%</td>
</tr>
</tbody>
</table>

**U.K. Sample**

The U.K. sample consisted of 1,048 participants. Survey results are not necessarily representative of the entire U.K. population, but the sample closely matches the age and gender distribution of the total population.

*Figure 6.4: U.K. Respondent Demographics*

<table>
<thead>
<tr>
<th></th>
<th>Sample Count</th>
<th>% of Sample</th>
<th>% of U.K. Population</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total</strong></td>
<td>1,048</td>
<td>100.0%</td>
<td>--</td>
</tr>
<tr>
<td><strong>Gender</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>520</td>
<td>49.6%</td>
<td>48.7%</td>
</tr>
<tr>
<td>Female</td>
<td>528</td>
<td>50.4%</td>
<td>51.3%</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18-24</td>
<td>126</td>
<td>12.0%</td>
<td>8.9%</td>
</tr>
<tr>
<td>25-34</td>
<td>187</td>
<td>17.8%</td>
<td>17.6%</td>
</tr>
<tr>
<td>35-44</td>
<td>163</td>
<td>15.6%</td>
<td>18.3%</td>
</tr>
<tr>
<td>45-54</td>
<td>177</td>
<td>16.9%</td>
<td>18.1%</td>
</tr>
<tr>
<td>55+</td>
<td>395</td>
<td>37.7%</td>
<td>37.0%</td>
</tr>
<tr>
<td><strong>Household Income</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Less than £10,000</td>
<td>65</td>
<td>6.2%</td>
<td>N/A</td>
</tr>
<tr>
<td>£10,000 to £24,999</td>
<td>237</td>
<td>22.6%</td>
<td>N/A</td>
</tr>
</tbody>
</table>

The Path to Digital Transformation: Controlling Friction While Tackling Cybercrime in Financial Services

<table>
<thead>
<tr>
<th>Income Range</th>
<th>Sample Size</th>
<th>Percentage</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>£25,000 to £49,999</td>
<td>398</td>
<td>38.0%</td>
<td>N/A</td>
</tr>
<tr>
<td>£50,000 to £74,999</td>
<td>139</td>
<td>13.3%</td>
<td>N/A</td>
</tr>
<tr>
<td>£75,000 to £99,999</td>
<td>71</td>
<td>6.8%</td>
<td>N/A</td>
</tr>
<tr>
<td>£100,000 to £149,999</td>
<td>40</td>
<td>3.8%</td>
<td>N/A</td>
</tr>
<tr>
<td>£150,000 to £199,999</td>
<td>7</td>
<td>0.7%</td>
<td>N/A</td>
</tr>
<tr>
<td>£200,000 or more</td>
<td>3</td>
<td>0.3%</td>
<td>N/A</td>
</tr>
<tr>
<td>Prefer not to answer</td>
<td>88</td>
<td>8.4%</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Sources: http://data.london.gov.uk; http://www.ons.gov.uk/

Sample includes respondents from across England, Scotland, Northern Ireland, and Wales.

**Figure 6.5: U.K. Respondents Regional Distribution**

Population Distribution
- England: 84%
- Scotland: 8%
- Wales: 5%
- Northern Ireland: 3%

Sample Distribution
- England: 85%
- Scotland: 9%
- Wales: 5%
- Northern Ireland: 1%

Sources: http://data.london.gov.uk; http://www.ons.gov.uk/

Note, respondents were not asked about their ethnicity due to market-specific sensitivities/restrictions.

Australia Sample

The Australian sample consisted of 1,029 respondents. The sample demonstrates a slight skew toward a middle-aged demographic in comparison to the total population, but is within the margin of error using a 98% confidence level. There is skewing toward a middle-income demographic of respondents, but with more than 10% of respondents opting not to state their income, definitive conclusions cannot be made about the survey demographics based on income segmentation.
Figure 6.6: Australian Respondent Demographics

<table>
<thead>
<tr>
<th></th>
<th>Sample Count</th>
<th>% of Sample</th>
<th>% of AU Population</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>1,029</td>
<td>100.0%</td>
<td>--</td>
</tr>
<tr>
<td><strong>Gender</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>489</td>
<td>47.5%</td>
<td>49.8%</td>
</tr>
<tr>
<td>Female</td>
<td>540</td>
<td>52.5%</td>
<td>50.2%</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18-24</td>
<td>117</td>
<td>11.4%</td>
<td>12.3%</td>
</tr>
<tr>
<td>25-34</td>
<td>173</td>
<td>16.8%</td>
<td>19.0%</td>
</tr>
<tr>
<td>35-44</td>
<td>208</td>
<td>20.2%</td>
<td>17.5%</td>
</tr>
<tr>
<td>45-54</td>
<td>197</td>
<td>19.1%</td>
<td>16.9%</td>
</tr>
<tr>
<td>55+</td>
<td>334</td>
<td>32.5%</td>
<td>34.2%</td>
</tr>
<tr>
<td><strong>Household Income</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Less than $25,000</td>
<td>85</td>
<td>8.3%</td>
<td>13.9%</td>
</tr>
<tr>
<td>$25,000 to $49,999</td>
<td>169</td>
<td>16.4%</td>
<td>21.6%</td>
</tr>
<tr>
<td>$50,000 to $74,999</td>
<td>187</td>
<td>18.2%</td>
<td>15.9%</td>
</tr>
<tr>
<td>$75,000 to $99,999</td>
<td>165</td>
<td>16.0%</td>
<td>13.3%</td>
</tr>
<tr>
<td>$100,000 to $149,999</td>
<td>183</td>
<td>17.8%</td>
<td>18.8%</td>
</tr>
<tr>
<td>$150,000 to $199,999</td>
<td>79</td>
<td>7.7%</td>
<td>9.0%</td>
</tr>
<tr>
<td>$200,000 or more</td>
<td>44</td>
<td>4.3%</td>
<td>7.4%</td>
</tr>
<tr>
<td>Prefer not to answer</td>
<td>117</td>
<td>11.4%</td>
<td>--</td>
</tr>
</tbody>
</table>


The Australian sample represents all areas of Australia, including Tasmania.

Figure 6.7: Australian Respondents Regional Distribution


Note, respondents were not asked about their ethnicity due to market-specific sensitivities/restrictions.
**Product Ownership**

Consumers were asked a series of financial product and device ownership questions for background and context. Respondents were required to indicate ownership of a checking account or debit card in order to complete the survey.

Respondents reported having an average of 3.8 different financial products. Penetration of core banking products (checking accounts, savings accounts, and debit cards) is—by design—relatively high across all three markets, although Australians were less likely to indicate ownership of a cheque account (and more likely to indicate ownership of a savings account).

*Figure 6.8: Financial Product Ownership*

<table>
<thead>
<tr>
<th>Product</th>
<th>U.S.</th>
<th>U.K.</th>
<th>AU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checking Account</td>
<td>78%</td>
<td>95%</td>
<td>41%</td>
</tr>
<tr>
<td>Savings Account</td>
<td>81%</td>
<td>79%</td>
<td>90%</td>
</tr>
<tr>
<td>Debit Card</td>
<td>87%</td>
<td>92%</td>
<td>88%</td>
</tr>
<tr>
<td>Credit Card</td>
<td>72%</td>
<td>75%</td>
<td>70%</td>
</tr>
<tr>
<td>Mortgage</td>
<td>32%</td>
<td>32%</td>
<td>35%</td>
</tr>
<tr>
<td>Other Loan</td>
<td>22%</td>
<td>16%</td>
<td>23%</td>
</tr>
<tr>
<td>Credit Monitoring</td>
<td>6%</td>
<td>5%</td>
<td>1%</td>
</tr>
</tbody>
</table>

**Segmentation**

Segmentation analysis was performed based on geographic, demographic, and behavioral attributes.

Market- and age-based segments are used throughout the report to highlight meaningful differences in consumer population sub-sets:
Figure 6.9: Respondent Distribution by Geographic & Demographic Segments

Market Segments

- AU: 33%
- U.S.: 33%
- U.K.: 34%

Age Segments

- 55 and Over: 34%
- Under 35: 30%
- 35 to 54: 36%

In addition to geographic and demographic segments, respondents were segmented based on the frequency with which they report shopping online, as an indicator of online engagement and account activity.

Figure 6.10: Respondent Distribution by Online Engagement Segment

“Over the period of a month, how often (on average) do you make purchases online or using your mobile device?”

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heavy</td>
<td>16%</td>
</tr>
<tr>
<td>Moderate</td>
<td>53%</td>
</tr>
<tr>
<td>Light</td>
<td>22%</td>
</tr>
<tr>
<td>None</td>
<td>9%</td>
</tr>
</tbody>
</table>

As expected, heavy and moderate online engagement skews toward younger consumers: 48% of heavily engaged respondents are under 35, compared to 16% of lightly engaged.
Figure 6.11: Online Engagement by Age

- **Heavy**
  - Under 35: 48%
  - 35 to 54: 31%
  - 55 and Over: 16%
- **Moderate**
  - Under 35: 36%
  - 35 to 54: 36%
  - 55 and Over: 33%
- **Light**
  - Under 35: 16%
  - 35 to 54: 49%
  - 55 and Over: 28%
- **None**
  - Under 35: 32%
  - 35 to 54: 49%
  - 55 and Over: 38%