

CONSUMER PERCEPTIONS
ON SECURITY:
DO THEY STILL CARE?

In 2014, **over 78 million records** containing personal information have been exposed in a breach¹. Even more alarming, **nearly 520 million financial records were stolen in the last 12 months**². There has been an epidemic of major data breaches in the last year, and with the increasing adoption of mobile and social platforms, consumer concerns about online security have grown.

In a survey commissioned by RSA and conducted by the Ponemon Institute, consumers generally perceive a loss of control over their personal information, however, they still believe security is important and expect it across digital transactions they perform. Despite high expectations for security, most consumers are still doing little to change their behavior.

This ebook explores the impact of data breaches on consumers, the effects of mobile on consumer behavior, and how consumers expect service providers to protect their digital identities.

¹ Identity Theft Resource Center, Data Breach Report, October 2014

² U.S. Federal Bureau of Investigation

DIGITAL IDENTITIES AT RISK

One in two consumers has received a notification that their personal information was lost or stolen at least once in the last two years.

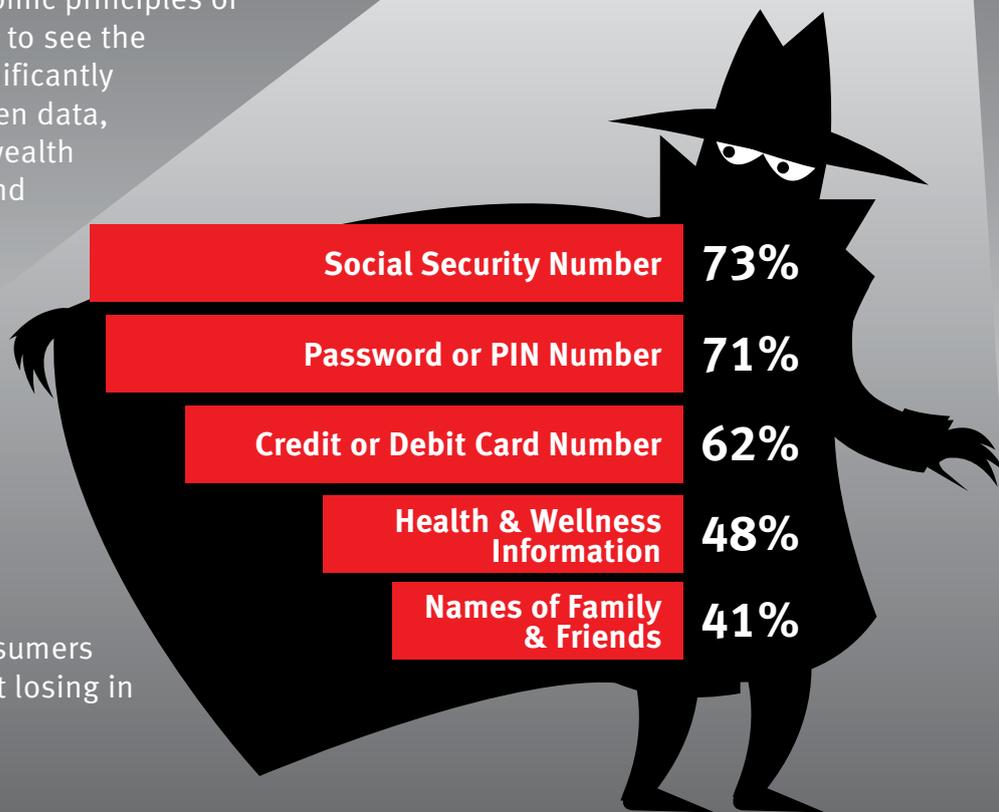
In addition, **77% of consumers** state it is very important or important that a service provider promptly notify them if their personal data is lost or stolen. Among the nearly one in four consumers who felt notification was not important, the majority, or **65%, cited the inability to stop fraud or identity theft as the top reason.**



STOLEN DATA IN THE BLACK MARKET

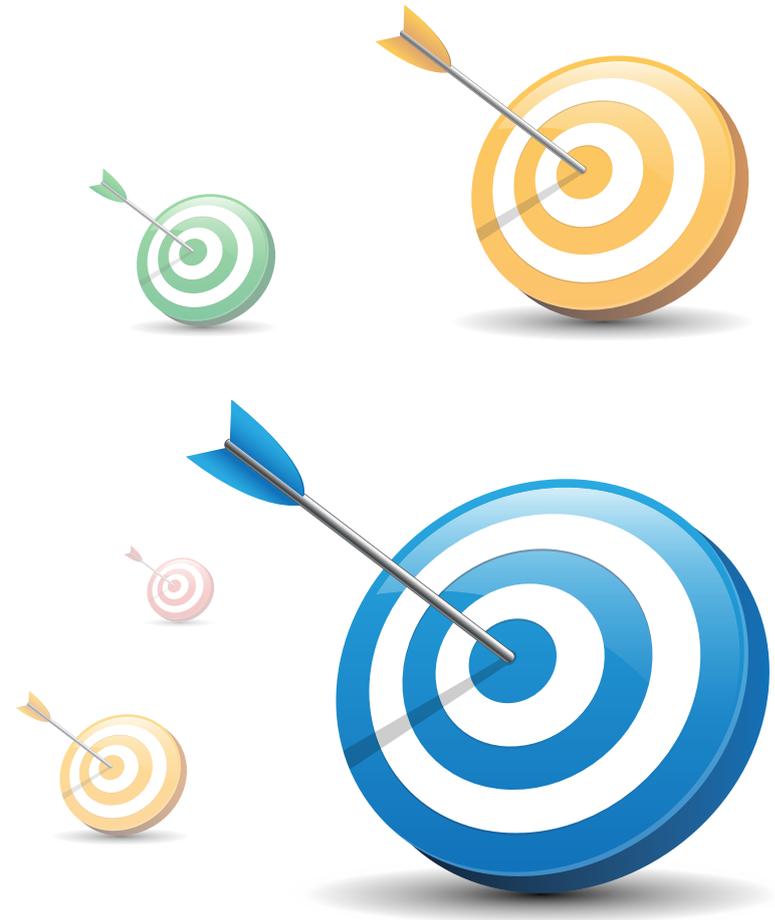
Just like a legitimate business, prices of stolen data in the black market follow the traditional economic principles of supply and demand. It is not uncommon to see the prices of stolen payment cards drop significantly after a major data breach. However, stolen data, such as medical records that contain a wealth of personal information, tend to command a much higher price. Regardless of the economics of the black market, consumers still tend to place the highest value on financial information.

Personal information consumers are most concerned about losing in a data breach (Top 5)



RETAILERS: THE NEW INDUSTRY TARGET

There has always been a general perception that cyber crime is an issue only for the financial industry. After a wave of high profile breaches targeting retailers, opinions are starting to shift. Changes are looming in the payment card industry as the U.S. becomes the last of the G-20 countries to embrace the EMV standard. With the wide adoption of EMV-enabled cards, it is expected that card-not-present fraud will grow exponentially. Early adopters of EMV technology in Europe experienced a high growth in card-not-present transactions as most fraud migrated to the online channel. The U.S. will be no exception. In fact, it is expected that card-not-present fraud will grow to \$6.4 billion by 2018³.

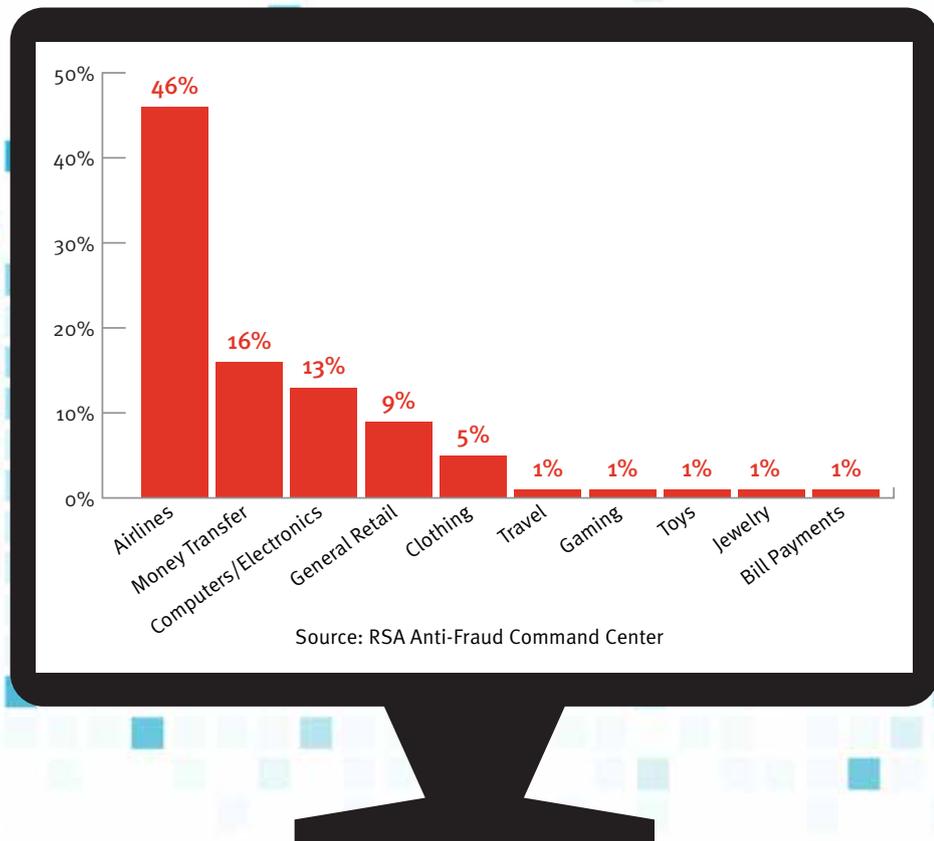


³ Card Not Present Fraud in a Post-EMV Environment, Aite Group, June 2014

E-COMMERCE FRAUD CONTINUES TO BE PREVALENT

The payment card industry will undergo significant changes in the next three years, which will have consequences for both retailers and financial institutions. However, e-commerce fraud is still a problem today with some merchants more affected than others.

Cyber criminals find it enjoyable to use stolen payment cards to indulge themselves with vacations, cash, and computers – and even to pay their monthly household bills. The following chart represents the top merchants affected by fraudulent transactions in 2014.



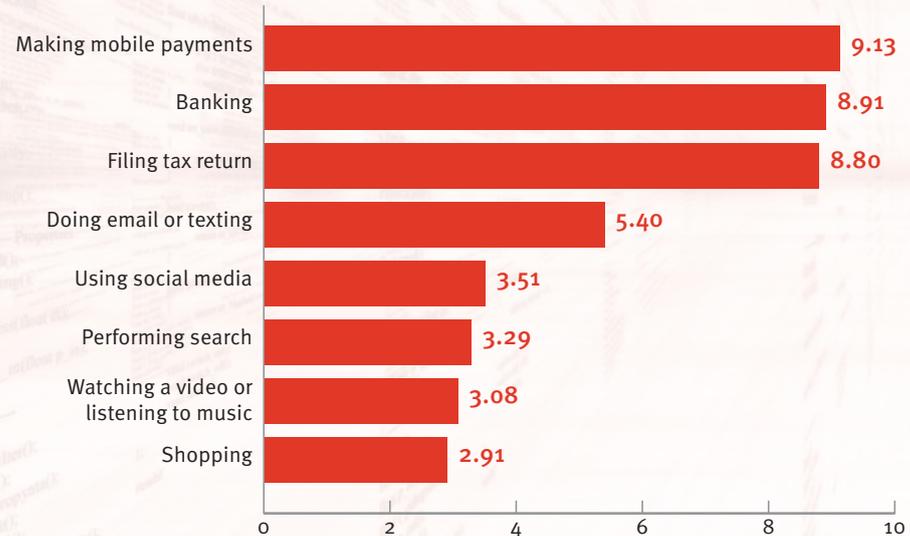
BREACHES DO NOT PACK A PUNCH WITH CONSUMERS

Consumers have remained relatively unaffected by the wave of retail data breaches involving the theft of payment card data in the last 12 months. Forty-five percent of consumers state recent breaches have not affected their use of credit or debit cards. According to the National Retail Federation, 44% of consumers plan to do their holiday shopping online, with a majority expecting to spend more than last year.

What is even more interesting is the level of security they expect based on the various online activities they perform. While it seems logical to expect consumers' expectations for security to be high for e-commerce due to so many retail breaches, it actually ranked the lowest on a scale of online activities, even below using social media and performing search.

Do you have an expectation of security when doing the following online activities?

1 = no expectation to 10 = high expectation



IN MOBILE WE TRUST - NOT!

The mobile channel is growing at unprecedented rates, surpassing even the adoption rates of the traditional online channel. And where the users go, cyber criminals follow. App stores are ridden with rogue applications, and malware once reserved for PC users is being developed to target mobile platforms. Even common cyber threats such as phishing are emerging in the mobile channel in the form of attacks delivered via text message. Smishing attacks, or SMS phishing, are highly successful due to the high open rates among mobile users and the general lack of consumer awareness surrounding this attack vector.

According to the survey, consumers feel a lack of trust in particular when it comes to mobile platforms. When asked about the mobile apps they download, 77% of consumers stated they do not trust the security of mobile apps. However, there is still a lack of concern as demonstrated by the more than 70 billion apps downloaded last year alone. In addition, only about one-third of consumers admit to actually reading the permissions requested by the apps they download.



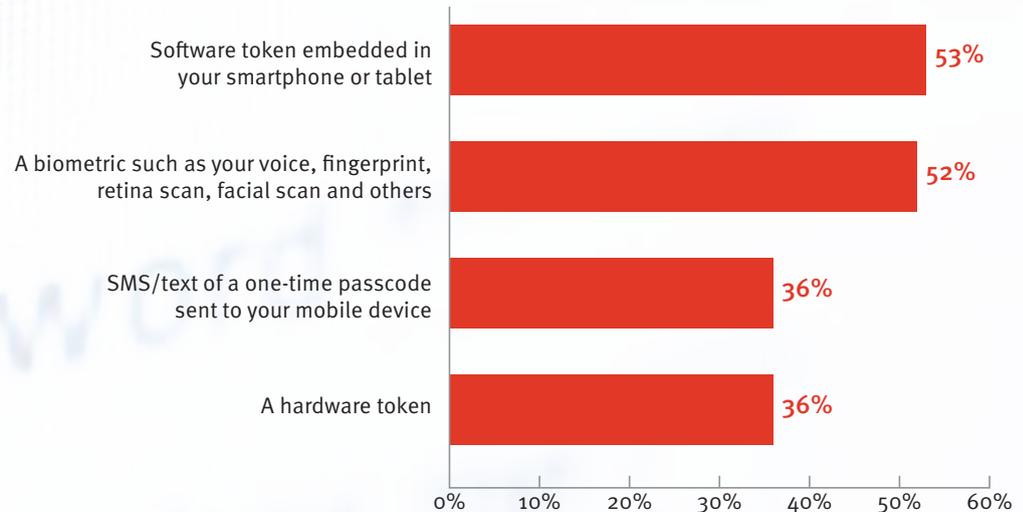
MOVE OVER PASSWORDS

62% of consumers state they do not trust websites that only rely on passwords to identify users, however about one in three use only one or two passwords across all the online accounts they access. As far as using personally identifiable information for verification, 78% of respondents say they would prefer authentication procedures that do not require them to share information such as a name, address, email and so forth.

New authentication methods seem to be catching on in the consumer space, however, as 53% of consumers find it acceptable for a trusted service provider to use biometrics technology to verify their identity. The most preferred methods outside of username and password include a software token embedded on a mobile device and biometrics such as voice verification and fingerprints.

Preferred methods to manage your identity online

(More than one response permitted)



A CALL FOR CHANGE IS COMING

While many consumers are doing minimal to change their behavior, they still place value in their personal information and have high expectations among service providers to secure their digital identities. Perhaps consumers have become desensitized to fraud and identity theft because so many have been affected, but they have still seen little change in many industries.

Financial institutions have enacted many security measures in the last decade to protect their customers which might explain the high security expectations that consumers have for banking providers. However, other industries have not been so quick to move. Passwords have been proven over and over to be ineffective protection against the flood of cyber crime that exists in today's digital world. However, there is still a prevalence of providers that use password-only security. This is only one example of disconnect when it comes to consumer security. The issue will only continue to exacerbate as organizations continue to move more services to the online and mobile channel – and even into the cloud.



EMC²

EMC², EMC, the EMC logo, RSA, and the RSA logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. © Copyright 2014 EMC Corporation. All rights reserved.

