DATA SECURITY IN 2014

Recent data breaches have renewed the debate over data security in the U.S. and have raised important questions. Amidst the debate, Americans spend *$3 trillion each year* safely and securely with their credit and debit cards.

And they have good reason to spend confidently: banks protect their customers by investing in infrastructure, technology and people to detect and prevent fraud, reissuing cards and absorbing fraud costs.

AMERICANS SPEND **$3 TRILLION EACH YEAR** **SAFELY AND SECURLY** WITH THEIR CARDS.

WHAT YOU NEED TO KNOW

Data breaches at major retailers such as Target and Neiman Marcus have raised questions about the security of your information and card accounts. Learn more about some common misconceptions about how your personal information is kept safe.

WHERE DO MOST DATA BREACHES OCCUR?

According to the Identity Theft Resource Center, in 2013, businesses, healthcare organizations, and educational institutions accounted for 86% of all data breaches. The financial industry accounted for 3.7%.

IS THE CUSTOMER OUT ANY MONEY AS A RESULT OF FRAUD?

Customers turn to their bank to make them whole when a retailer suffers a breach. Banks ensure the safety of your money and it's their common practice to immediately replace funds stolen due to fraud, providing the oft discussed "zero liability" when you use your card. It is not the entity (e.g. the retailer) that suffered the breach that immediately addresses your potential loss (it is only later that the breached party reimburses your bank and then only for a small percentage of the fraud.)

But banks' efforts also extend to taking additional steps such as reissuing cards and employing fraud-monitoring technologies, not to mention staffing up call centers to address customer concerns.

ARE THERE LAWS IN PLACE TO PROTECT CUSTOMERS?

Banks are subject to robust requirements under federal law that protect their customers' personal financial information from misuse. The Gramm-Leach-Bliley Act (GLBA) imposes stringent rules on how institutions must protect the security and confidentiality of such information with banks regularly examined for compliance by federal and often state regulators. Banks also adhere to regulators' Red Flag Rules, which require banks to implement a written Identity Theft Prevention Program designed to detect the warning signs of identity theft in their day-to-day operations. Moreover, Regulations E and Z along with network rules ensure customers are not liable for fraud if they notify the banks within a certain time period. As importantly, failure for banks to implement these rules can subject them to significant monetary penalties.

For merchants, there are no standard regulations or examination infrastructure comparable to what is in place for banks at the federal level to secure data or notify consumers. Merchants are subject to a myriad of state laws on the subject, though few if any impose standards requiring how they must care for consumer information. And, while merchants are supposed to comply with card network rules designed to guide retailers' efforts to build and maintain a secure environment, the largest merchants merely self-certify compliance.

IS THERE ONE SOLUTION THAT WILL GUARANTEE DATA IS PROTECTED?

The responsibility to protect consumers' personal information falls on many parties, and banks do all they can to protect consumers' data. However, there is not one solution or technology that is a panacea for fraud. The threats posed by cybercriminals are constantly changing, so it is important that everybody—banks, payment networks, merchants and consumers—work together to stay ahead of threats.

What we cannot do is focus on one solution that we hope will prevent future breaches. Today's threats are but a moment in time – there is a constant need to stay ahead of the ever-changing criminal threat, and that means embracing flexible approaches to solving both current and future challenges.

CONSUMER VIEWS ON DATA SECURITY

WHICH BUSINESSES ARE MOST RESPONSIVE TO DATA BREACHES?

A majority of Americans think companies do a good job of protecting their info. However, people think some types of businesses are more responsive than others in the event of a breach. People were asked how responsive different businesses are in the event of personal information being compromised.

Below is the percent of people who said they felt a business was very or somewhat responsive:

89% YOUR LOCAL BANK

83% CREDIT CARD COMPANIES

76% BIG BOX RETAILERS

76% DEPARTMENT STORES

67% SMALL BUSINESSES

48% SOCIAL NETWORKS

*"**92% OF PEOPLE** say that any company that has a data breach that could reasonably harm consumers should be required to publicly notify customers in a timely and effective manner."*

Source: Ipsos poll conducted on from May 27 - 29, 2014. For the survey, a national sample of 1,010 adults aged 18 and older from Ipsos' U.S. online panel.

IMPACT ON THE ECONOMY? DATA BREACHES CHANGE CONSUMER BEHAVIOR

Consumers have reacted differently to the heightened attention on recent data breaches. While three-fourths or more of customers either changed their pin or password or said they checked their bank and credit statements more frequently, there is evidence that recent data breaches may have an impact on the health of the economy.

Stopped shopping at a particular retailer they viewed as untrustworthy

Reduced or stopped making online purchases

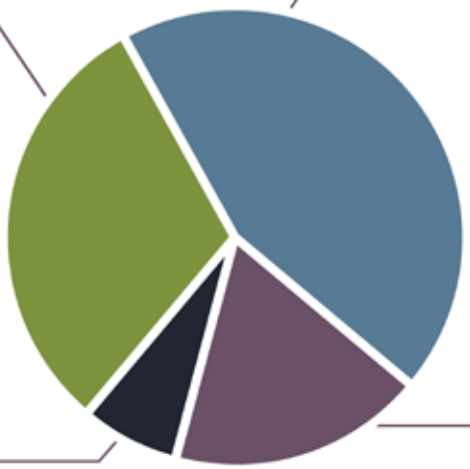
Reduced or stopped using their credit and/or debit cards

Source: Ipsos poll conducted on from May 27 - 29, 2014. For the survey, a national sample of 1,010 adults aged 18 and older from Ipsos' U.S. online panel.

ACCEPTING THE RISKS OF FRAUD? WHEN IT COMES TO THEIR PERSONAL INFORMATION:

31% say they know there are some risks with companies having access to their personal information, but they take these risks because of the benefits they receive.

7% say they are completely comfortable with companies having access to their personal information



44% say they know there are some risks with companies having access to their personal information, but with so much commerce taking place electronically they don't feel like they have any choice.

18% say they are uncomfortable with the risks of companies having access to their personal information and avoid most forms of electronic commerce.

Source: Ipsos poll conducted on from May 27 - 29, 2014. For the survey, a national sample of 1,010 adults aged 18 and older from Ipsos' U.S. online panel.

INNOVATING TO PROTECT CONSUMERS—A ROAD MAP FOR THE FUTURE

The banking industry, credit card networks, and others have come together to develop and introduce advanced technologies designed to provide consumers with robust protections against sophisticated cybercriminals. The future of protecting consumers is to implement a variety of technologies that will ultimately be the best safeguard against the ever-changing threats.

EMV Chips

EMV Chips: New EMV, or "chip" technology, involves embedding a microprocessor in plastic payment cards, mobile phones and other forms of payment that make the card nearly impossible to counterfeit and thus unattractive to the criminal element. Retailers and banks are already on their way to implementing this important change, with October 2015 set as the first date for rolling this out.

Tokenization

Tokenization: Tokenization technology replaces sensitive consumer information at the point-of-sale with a random "token," rendering the information useless to everyone except the merchant's card processor and the consumer's issuing bank. Expanded pilot programs are in motion in selected regions.

End-to-End Encryption

End-to-End Encryption: An important technology already being employed is end-to-end encryption, which uses sophisticated algorithms that encode a consumer's personal payment information into an unreadable form (and require a separate "key" to unlock it) as that information makes its way from a merchant's checkout stand to a card network to your local bank, and back.

Neural Networks

Neural Networks: Banks and credit card networks use sophisticated and complex systems and employ intensive training to fight against criminals looking to open accounts to use for fraudulent purposes. Neural networks are one type of system that banks use to detect unusual account activity, discovering that fraud may be at play. No doubt, many of us have received those calls from our card company asking about an irregular purchase. It is these robust systems, and banks' investments in them, that work to greatly protect consumers.

WORKING TOGETHER: BANKS, PAYMENT NETWORKS, PROCESSORS AND RETAILERS

Keeping data secure requires a collective effort of all involved: payment networks, banks, retailers, processors and new entrants in the payments space, many of whom are already hard at work combating an ever-evolving criminal threat.

Working together is critical which is why on February 13th, leading trade associations representing financial services and merchant industries announced a cybersecurity partnership that will explore paths to increased information sharing, better card security technology and maintaining the trust of customers.

Data security is a shared responsibility and this partnership works to ensure everybody does their part. Read more about the partnership ***here***.

PROTECTING YOUR IDENTITY: TIPS FOR CONSUMERS

Online commerce has exploded making it extremely easy for consumers to purchase goods. The benefits are immense but consumers must be aware of fraud, identity theft and other scams. The American Bankers Association recommends the following tips to keep users safe online:

- Keep computers and mobile devices up to date.
- Set strong passwords.
- Watch out for phishing scams.
- Forward phishing emails to the Federal Trade Commission (FTC)
- Keep personal information personal.

You can access more information visiting the ***ABA's Consumers Page***.

Have questions? Want more info? Contact Jeff Sigmund of the ABA at 202-663-5439 or *jsigmund@aba.com.*