

A low-angle, black and white photograph of several tall skyscrapers reaching towards a cloudy sky. The perspective is from the street level, looking up. A street sign for 'EXCHANGE PLACE' and a traffic light are visible in the lower left corner. A semi-transparent white horizontal band is positioned across the middle of the image, serving as a background for the text.

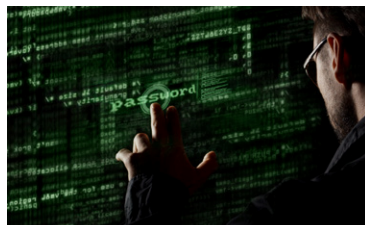
WHITE PAPER

Identity Theft and Account Takeover Fraud



Succeed. Transform. Compute. Perform.

Identity Theft and Account Takeover Fraud



Fraud from identity theft, account takeover and creation of new accounts continues to grow and has become a focus for financial institutions and their regulators, with losses estimated at \$5 billion a year.

EXECUTIVE SUMMARY

One of the many challenges and a top concern for financial institutions and their customers is dealing with financial fraud involving identity theft. According to the Association of Certified Fraud Examiners (ACFE) fraud against an organization can be committed internally by employees, managers, officers, or owners of the company, or externally by customers, vendors, and other parties.

Fraud experts rank identity theft as the fastest growing type of fraud as financial institutions continue to see increases in loss from account takeover fraud, credit card fraud and Internet fraud. Account takeover fraud continues to be a leading focus for financial institutions and their regulators.

ACCOUNT TAKEOVER FRAUD

Account takeover fraud occurs when an unauthorized party gains access to an existing bank account through identity theft and steals information from the account to conduct illegal transactions. The fraudster obtains and uses the victim's personal information to take control of existing bank or credit card accounts and carries out unauthorized transactions against them. Account takeover sequences can be initiated through various means. Most often, the consumer or an employee of the targeted business is lured into opening e-mail attachments or responding to social media friend requests, which often redirect the person to compromised websites. Account takeover activity differs from other forms of computer intrusion as the customer, rather than the financial institution maintaining the account, is the primary target.

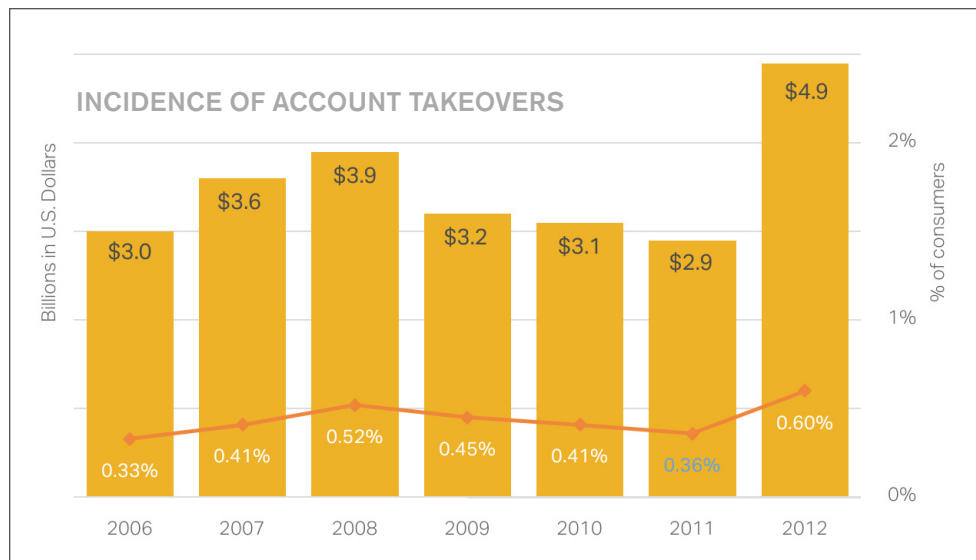
Cybercriminals may use phishing or spamming in order to gain access to the computer system. There are several methods of obtaining the account information depending on the ultimate goal of the intrusion effort. Trojan keystroke loggers are commonly used. This malicious software (malware) monitors and captures keystrokes including account access credentials and sends them to the cybercriminal to gain access to the account. This malware can be customized to target groups of individuals with the goal of accessing either financial or proprietary information. Once compromised, the criminal has access to the user passwords and credentials allowing him or her to control the system, transfer funds out, or gather and transmit data.

ANOTHER FORM OF IDENTITY THEFT IS APPLICATION FRAUD

This occurs when a perpetrator uses someone else's personal information to establish new accounts. Fraudsters employ a variety of techniques to obtain the personal and financial information typically needed to take control of existing accounts. According to law enforcement and fraud experts, obtaining such information can be as simple as dumpster diving or cold calling. Alternatively, fraudsters may use more technology-reliant methods, such as phishing, or establishing fake websites to collect payment details. Incidents of application fraud are increasing in both frequency and levels of financial loss.

While account takeovers are most often achieved through the use of malware that exploits just one entry point into a network to start the theft, fraudsters may also use social interaction to prompt individuals into divulging account information. This information allows the fraudsters to access the account and move the money out of the account in a very short time. A 2012 Javelin study estimated losses from account takeover

fraud at over \$4.9 billion, representing a 69 percent increase over 2011. The same study concluded that much of this increase is likely attributable to security vulnerabilities in online and mobile channels, as well as shifts in consumers' use of technology. This \$4.9 billion in losses includes other consumer accounts such as loans,



October 2005 through 2012 n = varies 4,784-5,249 Base: all consumers
Data from 2013 Javelin Strategy & Research

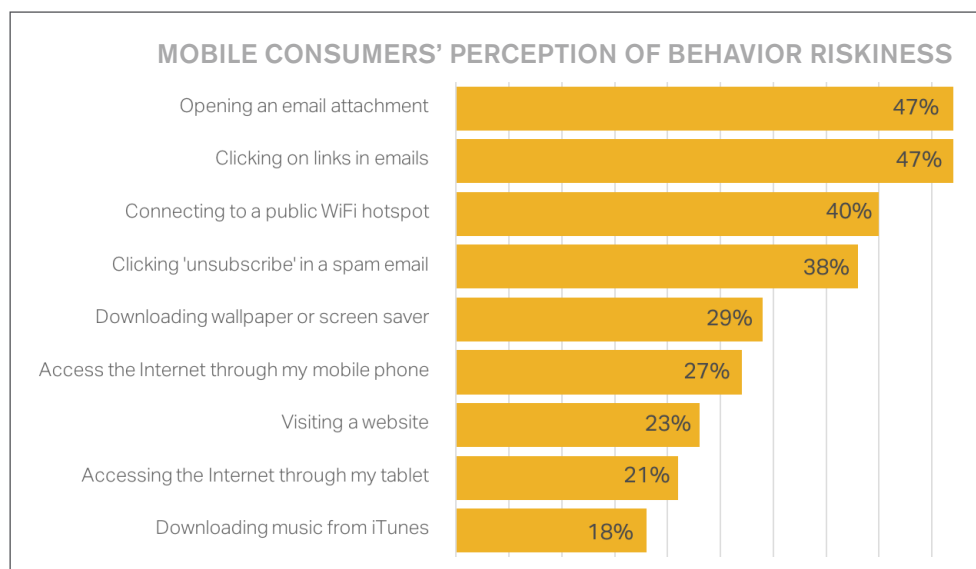
insurance, telephone, and utilities—in addition to deposit accounts at financial institutions. The data above illustrates the growing incidence of account takeovers.

Sources:

2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters.
Javelin Strategy & Research, February, 2013.

Account Takeover Activity, Department of the Treasury Financial Crimes Enforcement Network Advisory notice (FIN-2011-A016), December 19, 2011

The Javelin study also revealed that as new technology evolves and solutions emerge to successfully mitigate some forms of account takeovers, criminals have shifted their attention to less defended targets such as mobile devices. Mobile devices provide fraudsters with a variety of ways by which to compromise the data stored or transmitted by those devices, thus opening additional doors to account takeovers.



As depicted above, less than 50 percent of consumers see risks from otherwise dangerous behaviors when used in a mobile environment.

Source: 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters. Javelin Strategy & Research, February 2013.

From a cybercriminal perspective, it's just as easy to access a financial institution or business account through a mobile text or e-mail as it is through a computer. While free antivirus applications are available and can help protect against many of these scams, educating the user on the vulnerabilities and risks of not having antivirus protection should be on the forefront as one of the most effective defenses against account takeover fraud.

PROTECT AGAINST IDENTITY FRAUD

Some useful methods to protect against identity fraud:

- ☐ Always check bank and credit card statements for inaccuracies.
- ☐ Check your financial information regularly, looking for what should and should not be there.
- ☐ Order and check your credit report at least once a year.
- ☐ Before providing personal information, make sure the individual or business requesting it has a valid reason for requiring the information.
- ☐ Never write your credit card numbers or Social Security number on checks or on the outside of envelopes.
- ☐ Do not put your Social Security number on any document unless you are legally required to do so.
- ☐ Do not give account numbers over the telephone or to persons/companies you are not familiar with.
- ☐ Do not use cordless or cellular telephones or e-mail to transmit financial or private personal information.
- ☐ Keep all financial documents in a secure place.
- ☐ Choose passwords that will be difficult to crack and use different passwords for all accounts.
- ☐ Change passwords and PIN codes often.
- ☐ Use different PIN numbers for all of your cards.
- ☐ Do not store your PIN numbers on mobile phones or laptops.
- ☐ Make sure your computer security (spam filters, virus protection, firewall, passwords, etc.) is robust and up-to-date.

Sources: [http://ithandbook.ffiec.gov/it-booklets/supervision-of-technology-service-providers-\(tsp\).aspx](http://ithandbook.ffiec.gov/it-booklets/supervision-of-technology-service-providers-(tsp).aspx)
Cybersecurity Assessment Tool, <https://www.ffiec.gov/cyberassessmenttool.htm>

SUMMARY

As technology advances and continues to rapidly connect more and more people around the globe, the growth in connectivity, convenience, speed, technology adoption, and online and wireless payment options make it easier and more efficient than ever for individuals and businesses to conduct financial transactions. These same factors have given rise to new forms of fraudulent activities such as account takeover and other transnational crimes which are difficult to detect and prosecute.

Companies are encouraged to continuously assess and examine their information security standards, systems of internal control, policies and procedures in order to better identify, measure, monitor, control and report on weaknesses which could be exploited by management, employees, vendors or outside perpetrators.