THEFRAUDPRACTICE
INNOVATIVE STRATEGIES FOR ECOMMERCE PAYMENTS & FRAUD PREVENTION

Many Businesses Are Unprepared for the Growing Risk of Account Takeover

Press release dated 6/5/2013, By David Montague The Fraud Practice LLC,

We are starting to see more and more fraudsters focusing larger efforts on using account takeover (ATO) to perpetrate fraud. Most likely it is because businesses aren't focused on account takeover (ATO) risk today and there is a vast supply of compromised consumer and business accounts from cases of phishing, pharming, malware and data breaches. Any business that offers users the ability to setup an account or protects their customer information behind a login is at risk to account takeover (ATO) and a potential target for fraud.

"There is a broad misconception in the market that ATO is really only a problem for financial institutions. In fact, the data indicates that fraudsters have already turned their attention away from financial institutions and have merchants and e-commerce providers squarely in their sights. By some accounts, ATO has already eclipsed the damage caused by credit card fraud in hard dollar terms." Michel Glasson, CEO NuData Security Ltd

The issue is many businesses do not know the extent of their exposure to account takeover nor do they know how to measure the presence of account takeover attempts, and most importantly they do not know the best practices on how to protect their business and customers from account takeovers.

"The problem is most companies are blind to ATO signals which is why NuData Security developed a service like NuDetect, a behavioral analytics service, to help companies detect ATO and other automated fraud activity. We firmly believe to successfully detect and prevent ATO from occurring companies will need tools to be able to monitor consumer behavior across key events." Michel Glasson, CEO NuData Security Ltd

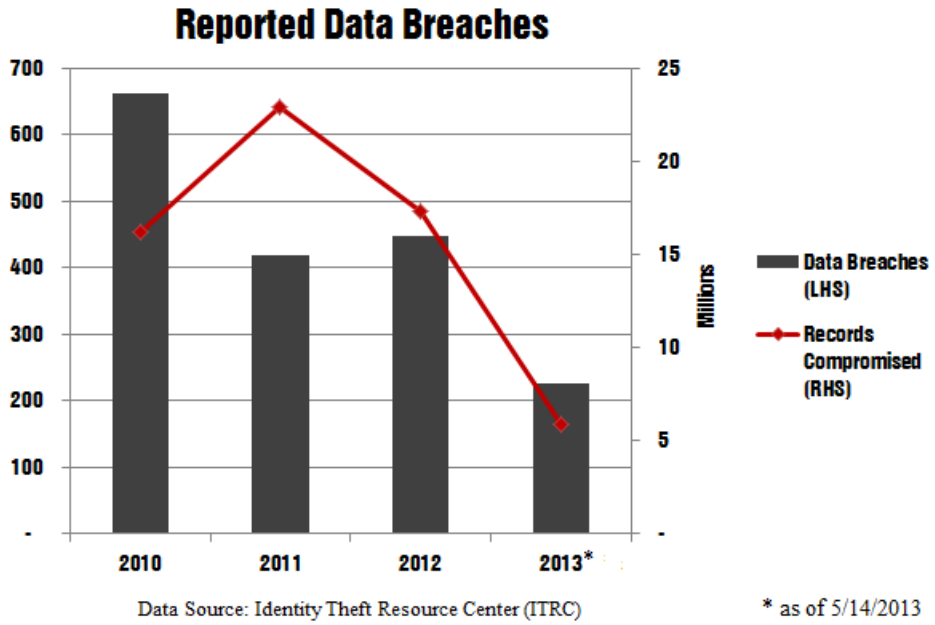
There is no denying that account takeover has been a growing issue for fraud and risk management. The Federal Reserve Bank of Atlanta recently published a document making the case for greater education of consumers and employees as a means of mitigating online account takeover risks. The report also references a recent study from Javelin Strategy and Research showing that account takeover dollar losses in the United States increased by $2 billion from 2011 to $4.9 billion in 2012, a 69% increase, victimizing 0.6 percent of all U.S. consumers. But account takeover isn't just increasing in the United States. According to CIFAS, a non-profit membership association focused on fraud prevention in the UK, account takeover fraud incidences increased 53 percent in 2012 to where account takeover now represents 65 percent of all identity related fraud in the United Kingdom.

One of the primary reasons account takeover fraud has been increasing is because fraudsters are able to get their hands on ever increasing account credentials through successful efforts at scaling data breaches, phishing and pharming activities. Account credentials and compromised data records remain at high levels while phishing and pharming continues to increase and evolve. As reported by Financial Fraud Action UK, an offshoot of the UK Payments Administration, there were over 111,000 pharming sites spoofing UK banks and building societies identified in 2011. Meanwhile RSA identified over 27,400 phishing attacks worldwide with 257 different brands being targeted just for the month of February 2013. Meanwhile, phishing and pharming tactics are morphing to target social

media users. Symantec stated in their 2013 Internet Security Report that phishing attacks via email have declined, but at the expense of more phishing scams carried out through social networking platforms like Facebook and Twitter. The study additionally found that pharming sites spoofing social networks increased by 123 percent in 2012.

While phishing, social engineering and other schemes trick consumers into providing their account credentials, data breaches can affect thousands and sometimes millions of consumers in a single attack. Although data breaches involving Social Security Numbers and payment account information can do the most immediate financial harm, breaches involving email addresses, usernames and passwords can lead to high losses as well. Due to the fact that consumers tend to reuse usernames and passwords across sites so an account compromised with one business can be used to takeover accounts with other companies or services.

With the continued high level of data breaches and compromised records in recent years, many online organizations that did not suffer a breach directly have been concerned about the potential fraud risk they might incur from other companies compromised data and accounts. The Identity Theft Resource Center tracks all reported data breaches and tallies the number of compromised records, while noting that there is likely a significant number of data breaches that go unreported. With over 400 data breaches and tens of millions of records compromised in each of the past three years, fraudsters have plenty of information to use for attempting account takeover. So far this year data breaches have been keeping pace with 225 reported incidences and nearly 6 million compromised records recorded by the IRTC as of May 14, 2013. This does not include the 50 million emails and passwords compromised with the recent LivingSocial data breach.



The threat of account takeover is continuing to rise, and it affects all varieties of online organizations to include merchants of all types, financial institutions, social networks as well as the telecom, utilities and insurance industries. Preventing account takeover can be difficult, especially when a

consumer has handed over their login credentials or has reused passwords that were compromised in a data breach elsewhere. But there are several things organizations can do to mitigate this risk.

The first step is understanding the vulnerabilities that make a company more susceptible to account takeover. There are many factors that contribute to account takeover risk ranging from password policies to use of bot protection and other tools or features to reduce ATO risk. Organizations also need to understand their potential risk exposure from account takeover, that is, understanding what they are protecting behind a user login, how valuable this information is and how easily it can be monetized or used directly to make purchases or transfer funds.

As a company you need to ask yourself a series of questions to understand how at risk you are to account takeover ATO. Do you manage accounts for your customers? Do you know your vulnerability to account takeover ATO? Do you know your exposure to account takeover if it occurs? Can you measure and monitor for the presence of account takeover? Keep in mind, when it comes to ATO vulnerabilities, many go unnoticed by businesses until they are exposed when account takeover becomes the basis of a significant loss event. Even with significant account takeover losses and events taking place, how these are being perpetrated and what can be done to correct this may still be unknown for many businesses. If you are struggling to answer these questions, or in developing a strategy to deal with ATO consider an Account Takeover ATO audit.

For more information:

Account Takeover Risk Audits from The Fraud Practice
Mitigating Online Account Takeovers: The Case for Education – The Federal Reserve Bank of Atlanta
ID theft drives fraud to new levels in UK (CIFAS)
Financial Fraud Action UK – Fraud the Facts
Identity Theft Resource Center (ITRC) – Reported Data Breach Statistics