How Online Identity Fraud Harms Businesses and What You Can Do About It

An Osterman Research White Paper

Published April 2014

SPONSORED BY
e-hawk
ONLINE IDENTITY FRAUD IS ATTACKING YOUR BUSINESS

Criminals and other bad actors are rapidly evolving their online identity fraud techniques to move quickly and commit their crimes. More hackers and bad actors are attacking enterprises than ever before, fueling a sense of urgency around finding timely solutions to reduce risk for online services, credit card processors, e-commerce merchants and consumers. Consequences include:

- Cybercriminals signing up for new accounts using fraudulent information including bogus user names, email addresses, and domains. This access readily attacks against online service providers and can quickly damage a trusted brand’s reputation.
- Bad Actors hijack legitimate registered customer accounts using valid customer login and password data. All for unlawful purposes such as sending high volumes of spam to distribute malicious software or phishing scams designed to defraud consumers of financial information by masquerading as a trustworthy entity.
- Organized thieves employ stolen financial assets including credit card numbers and account information to place orders for goods or services.

Online identity fraud impacts revenue and customer growth, and can seriously damage reputation, brand image, and halt expansion into new markets. The FBI classifies a stolen identity as a powerful cloak of anonymity for criminals and terrorists...and a danger to national security and private citizens alike.

WHO IS AFFECTED?

Online identity fraud impacts a wide range of online service providers and other organizations:

- Providers of digital goods, those with nearly instantaneous delivery, such as computer software downloads; eGift cards; travel services; eTickets for entertainment events; music and other downloadable digital media; digital items within games and social networks, etc.
- Providers of digital services, such as cloud-based email services, CRM services (e.g., Salesforce.com), ERP services, cloud-based storage, and online broker services such as Airbnb and Uber.
- Sellers of physical goods that maintain an e-commerce site, such as Amazon, eBay, Craigslist or any of the hundreds of thousands of other online retailers worldwide.
- User-generated content sites that provide ratings and reviews, such as Yelp, OpenTable, Angie’s List, Citysearch or Yahoo! Local Listings.
- Any of the 1,000+ social networks in use worldwide – such as Facebook, Twitter or LinkedIn – that can be used by cybercriminals to distribute spam or links to malware-focused sites and, through the use of social engineering, can easily infect legitimate users.

ABOUT THIS WHITE PAPER

This white paper discusses the growing problem of online identity fraud, what organizations should look for in a fraud reduction solution, and several use cases that describe how organizations have been able to reduce online identity fraud. The paper also provides a brief overview of E-HAWK, the sponsor of the paper, and its relevant solutions.
ACCOUNT IDENTITY FRAUD IS A SERIOUS ISSUE

WHAT DO BAD ACTORS DO?
There are a variety of methods employed by cybercriminals to commit online fraud, some with more damaging and far-reaching consequences than others. Here are a few examples of how bad actors use online identity fraud for financial or other gain:

• **Exploit the “freemium” model**
  There are literally thousands of “freemium” services available – services that provide useful functionality, but with limits on features, functions, storage or other capabilities. Providers offer these services with the hope that customers of the free service will purchase more capable versions of these offerings once the freemium version has sold them on the benefits of the services.

  Cybercriminals often register for these services and use them for nefarious purposes. For example:

  • In one exploit, cybercriminals distributed a bogus memo purportedly from the Association of Southeast Asian Nations (ASEAN) that was sent using a Dropbox notification message. When the victim opened the Dropbox-hosted Microsoft Word document, embedded malware in the file communicated with a Wordpress blog site (another freemium service) that carried out additional commands.

  • Cybercriminals have used Google Docs to infect spear phishing victims with malware using Google Docs’ actual SSL capabilities. The document to which users are directed is a legitimate, but stolen, Google Docs document.

The benefit to cybercriminals of using freemium services is that their use lends an air of legitimacy to phishing and spear phishing campaigns because of the social engineering aspect of the attack. For example, when potential victims see a Dropbox link in an email they are more likely to click on the link than if it references a random URL. More seriously, however, when paid versions of freemium services become well established in an organization, as is the case with Dropbox and many other widely used services, these services can get whitelisted by IT, resulting in cybercriminals’ easier access to users through corporate firewalls.

• **Gain access to e-commerce sites**
  Another common result of online identity fraud is that cybercriminals can register with e-commerce sites and purchase products using stolen credit cards. Stolen cards sell for relatively little on the black market – stolen MasterCard numbers, for example, were selling for anywhere from $26.60 to $44.80 each as of late December 2013, although prices before the well-publicized Target breach were upwards of $100 per card.

  Credit card numbers can be stolen through a variety of means, including direct hacking attacks, keystroke loggers, botnets, credit card skimmers and other means. Card numbers can then be used to purchase from online retailers or, in some cases, physical stores. In some cases, dishonest individuals who work in affiliate marketing programs will use stolen credit cards to generate bogus sales.

Case Study: MailChimp
MailChimp is a leading provider of newsletter-delivery services, serving more than five million users worldwide.

MailChimp recently implemented E-HAWK and is very pleased with the results it has seen so far. MailChimp often sees a large number of spammers attempt to sign up for the service, and with E-HAWK, entire groups of spammers have “simply gone away”.

At present, MailChimp uses E-HAWK primarily in a manual mode to weed out high-scoring bad actors, and plans to automate the process in the near future. The positive results have given MailChimp a significant degree of trust in E-HAWK, particularly the company’s willingness to fine-tune its algorithms to meet MailChimp’s requirements. A senior decision maker with MailChimp noted that E-HAWK “empowers our compliance group to quickly identify bad accounts we have not seen before and would not catch”.

©2014 Osterman Research, Inc.
How Online Identity Fraud Harms Businesses and What You Can Do About It

in order to earn a commission from the affiliate program. The process of using stolen credit cards is made substantially easier by many consumers’ propensity to over share on social media and other sites, making it relatively easy for cybercriminals to obtain necessary information about the owners of the stolen credit card information they possess.

- **Leverage social media to scam others**
  Another type of cybercrime involves signing up for social media accounts using false information; or copying someone else’s profile, blocking the actual owner from seeing it, and then asking all of the real owner’s friends to accept their friend request.

Many social media operators have experienced a significant penetration of fake followers – for example, the most-followed Twitter account is that of Katy Perry who has 51.5 million followers as of mid-March 2014, 31% of which are bogus. One analysis found that there were 20 million fake Twitter accounts as of summer 2013, or roughly nine percent of Twitter’s active users each month. Facebook estimates that in 2013 between 67.7 and 137.8 million of its accounts (5.5 percent to 11.2 percent were fake), although “only” 4.9 million to 14.8 million (0.4 percent to 1.2 percent) were accounts that were created in violation of Facebook’s acceptable use policy.

Cybercriminals who create these bogus accounts can use them to distribute spam to followers or friends, or otherwise scam the individuals who follow them in a variety of ways.

- **Use bidding and auction sites for criminal purposes**
  Another common form of cybercrime is seller misrepresentation on online auction sites like eBay, QuiBids, eBid, OnlineAuction or WebStore. This is a fairly common type of cybercrime – in fact, the Internet Crime Complaint Center (IC3) reports that online auction fraud is the most common type of Internet-based crime in Romania.

- **Register for contests with bogus information**
  Another fairly common technique used by cybercriminals involves registering for contests with the goal of winning some sort of cash or other prize in exchange for “Liking” a Facebook page, providing contact details as part of a prospecting program, or simply getting attention. However, these contests are almost always flooded with bogus entries in addition to the valid entries that the content sponsor hoped to acquire.

In one such case, a social media consultant helped a US-based business to run a contest on Facebook in which contestants were asked to send in pictures of sleeping babies – the winner would earn a $150 gift card to Target. However, the contest generated a large number of bogus entries, many of which were from Bangladesh. However, there have been more serious examples of contest fraud:

- Coca Cola’s “2011 Twist Txt Win Sweepstakes” offered a number of prizes to individuals who texted winning codes printed on the underside of Coca Cola product bottle caps. Between May and September of 2011, a mother and daughter in western Oregon were able to “win” between $40,000 and $200,000 in prizes. The pair was caught and charged with computer crime, aggravated theft and identity theft.

- In early 2012, Taco Bell ran a promotion that offered customers the opportunity to win a PlayStation Vita game system. However, four days after the promotion started, Taco Bell’s network operations team detected significant spikes in entry activity that indicated fraudulent entries.

- Kmart ran a contest in 2010 in which it would give out 5,328 $20 gift cards to individuals who were permitted to provide an entry once each day.
However, the contest was suspended when bot activity was discovered, allowing some individuals to provide their entry hundreds of times per day\textsuperscript{xii}.

According to Gartner, "Social engineering schemes and scams are also targeted directly against consumers, and these often impact the financial institutions where consumers keep their money. For example: Singles on dating sites fall for solicitations from criminals who are posing as suitors\textsuperscript{xi}".

THE CONSEQUENCES CAN BE SERIOUS
The consequences of illegitimate signups for freemium services, fake customers, fake social media accounts and other bogus activities can be quite serious and, in some cases, can threaten the longevity of a business. For example:

- Bogus customers can result in loss of funds and loss of revenue from an increased number of chargebacks or bad debts from "customers" who use stolen credit cards. At a minimum, the result for an online merchant can be a slew of cancelled orders from individuals whose fake identity is discovered before the order is processed and product is shipped.

- Online identity fraud can also result in significant damage to an organization’s or brand’s reputation because of reduced traffic quality, negative press reports, lower signup rates from bona fide customers, and an increase in customer complaints. For example, a valid social media account holder whose identity is stolen by a cybercriminal may opt not to use the service in the future. This is particularly troublesome for service providers whose paying customers may switch to another service after having their account hijacked.

- Bogus leads can waste corporate resources because salespeople will spend time following up with fake or non-compliant leads. Moreover, the response time in reaching valid prospects will be slower because of the sometimes-significant number of illegitimate contacts that sales personnel must eliminate.

- Ultimately, online identity fraud can erode customer and prospect confidence in an organization or brand, reducing the potential value of the customer base as defrauded customers leave a service or are more reluctant to sign up unless additional incentives are offered.

- According to IBM’s estimates, companies lose $3.5 trillion annually to fraud, which is 5% of the world’s total GDP\textsuperscript{xiv}. Forrester Group reports "Fraud costs are soaring to such an extent that no organization can consider it an acceptable ‘cost of doing business’ anymore. With 80% of fraud committed by fraud rings and networks of fraudsters, it has become increasingly clear to firms and vendors that they cannot fight fraud rings effectively as singular entities\textsuperscript{xv}."

---

**Case Study: Campaign Monitor**

Campaign Monitor is a nine year-old company with 800,000 users of its email campaign management solution. The company is adding roughly 5,000 new customers every week.

Campaign Monitor began using E-HAWK in late 2013 and has been aggressive in its scoring of potential customers in order to weed out bad actors to the greatest extent possible. The goal in taking this approach is not to waste pre-sales resources on bogus sign-ups and the strategy has worked quite well. Campaign Monitor has seen an enormous decrease in the number of spammers (Bad Actors that intend to send high volumes of unwanted email messages and then not pay) who signing up for their service.

To evaluate E-HAWK, Campaign Monitor ran a test on 20,000 accounts that had been denied access to their system, as well as a second group of 5,000 verified, valid accounts. E-HAWK performed very well in both tests.

Campaign Monitor has been very pleased with the performance of the system and, to date, has not experienced any “false positives” – a valid customer that was denied access to the system improperly. Moreover, the use of E-HAWK has enabled a significant reduction in the amount of manual work required to vet new customers. In fact, an unexpected side benefit of E-HAWK’s solution has been that they can now identify valid users who had incorrectly entered their email address.
PROBLEMS GET WORSE AS COMPANIES GO DOWNMARKET
The problems with online identity fraud become worse as companies go down market to generate new business. Because there are more prospective customers available as companies market to smaller prospects, but typically lower profit margins to be generated by selling to them, there are fewer resources available to detect online identity fraud on a per-customer basis. The result can be a much higher incidence of bogus registrations, fake leads or non-valid sales when selling to smaller prospects. This, in turn, can result in a significant increase in chargebacks, lost revenue and brand damage.

WHAT ORGANIZATIONS SHOULD LOOK FOR IN A FRAUD REDUCTION SOLUTION
There are a number of best practices and feature sets that organizations should look for as they seek to score/vet prospects and thereby reduce online identity fraud:

• Use a layered and redundant approach to fraud protection. This should include the use of multiple data sources, platforms and checkpoints to identify potential bad actors, since no one platform can hope to solve the entire issue of online identity fraud. For example, a robust scoring/vetting solution should examine a large number of attributes for a prospective signup, customer, etc. and assign scores to these attributes. Depending on the value of the access, service or product that the prospect seeks to acquire, the attributes to be checked and correlated could be the location of their IP address, the domain name of their email account, their address, their telephone number, the frequency of their signup activity and any community history that might be available.

• Community-based data sources of known fraudsters should be leveraged to the greatest extent possible so that vendors and other providers can use the collective experience of their peers facing the same problems of fraud. According to Forrester Group, “using a cloud-based fraud management product not only eases the pain of operations and model updates but also can provide up-to-date consortium data that allows for real-time fraud prevention at a lower cost”xvi.

• Barriers to fraudsters should be created by redundant testing using multiple data sources. Any fraud reduction solution should be based on robust data analysis, as well as solutions from multiple sources and testing, since a combined analysis produces the best results in detecting and preventing fraud.

• Any scoring approach must minimize the number of false positives (valid customers identified as risky) and false negatives (bogus customers identified as legitimate). One benefit of a robust scoring/vetting solution is that it will identify potentially risky customers and offer to them a reduced feature set or privileges until the customer has been more thoroughly vetted.

• The scoring and vetting of prospects, signups and others must be conducted at very low cost, particularly as companies seek to go down market and generate a larger number of customers with tighter operating and profit margins.

• Ideally, any scoring/vetting system will integrate with existing CRM, ERP or other solutions and allow the use of rules to determine how leads, signups, prospective and actual customers are managed. For example, if someone signs up for a freemium service, but then changes their contact information, the system should allow the account to be locked if high-risk information is detected.

• Finally, the solution should minimize any negative impacts for bona fide customers, such as excessive wait times before access is granted or denied, and it should eliminate the use of CAPTCHAs and other onerous mechanisms to the greatest extent possible.
The primary goal in account fraud detection is to score prospects, customers and users in order to identify likely bad actors, but to do so in a way that does not impact the ability for valid customers to gain access to the features and functions of the services being offered, or that interferes with legitimate customers’ ability to conduct business with a company. The benefits of scoring and vetting prospective customers, and thereby identifying potential bad actors, are several:

- By limiting capabilities, features and functions for risky users, the likelihood of online systems being used for scams or fraud is minimized.
- E-commerce fraud can be reduced along with the various problems it creates, including chargebacks and cancelled orders.
- Corporate reputation can be enhanced as prospective customers become aware of the safety of doing business with a firm that carefully vets its prospects and eliminates fraudsters to the greatest extent possible.

**WHAT YOU NEED TO KNOW**

Online identity fraud through bogus registrations, signups, contest entries and product purchases is an enormous problem that can impact an organization financially and also do long term damage to reputation and brand. To minimize the impact of online fraud, organizations should implement a system to vet prospects and score them based on their risk. Any such solution should use a multi-layered approach and evaluate a large number of data points, attributes and content sources as part of the scoring process. Moreover, scoring and vetting of prospects should be managed as inexpensively and as unobtrusively as possible.

**ABOUT E-HAWK**

E-HAWK is a technology innovator in the Web & Mobile Fraud Detection & Prevention space. They make heroes out of Online Risk/Fraud Managers because they deliver a world-class solution that provides quality, actionable cyber intelligence to help combat fraudulent transactions, registrations, and account hijacking to combat organized cybercriminals. The company launched in 2012 and began offering a user vetting service to help identify risk profiles of account registrations and profile updates in real-time. E-HAWK has vetted over six million users, identified hundreds of thousands of bad actors, and is helping prevent cyber theft across multiple sectors, including financial services, online retail, travel, ticketing, entertainment, social networking and gaming.

E-HAWK is also a trusted source for community data on known bad actors shared by customers for the sole purpose of helping everyone in the community combat active known fraudsters. Cybercriminals tend to attack multiple organizations and leave a trail wherever they go. The company’s platform can provide rapid identification and stop Bad Actors from being able to inflict damage on multiple businesses. Their community of trusted Email Service Providers (companies providing email marketing services on behalf of clients), Internet Service Providers (companies providing services for accessing, using, or participating in the Internet), and global online businesses contribute information on cyber criminals verified as Fraudsters. This anonymous pooled data is used to stop bad actors from inflicting damage on multiple accounts.

For more information, visit www.e-hawk.net.
How Online Identity Fraud Harms Businesses and What You Can Do About It

© 2014 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader’s compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, “Laws”)) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

REFERENCES

5. Analysis by StatusPeople run on March 18, 2014.
15. Forrester Group, Forrester’s Quick Take: IBM Announces A Streamlined Fraud Management Portfolio
16. Forrester Group, Big Data In Fraud Management Variety Leads To Value And Improved Customer Experience