GT GreenbergTraurig

Alert | Retail/Data, Privacy & Cybersecurity

May 2019

# Retailers: Protecting Against Credential Stuffing Attacks

It is no secret that the retail industry has suffered many devastating blows due to sophisticated cybersecurity attacks. Recently, retailers have been facing a new threat – "credential stuffing" attacks – in which hackers use stolen email addresses, user names, and passwords to attempt to break into corporations. So far in 2019, several large companies have suffered these attacks (some, multiple attacks).

Most recently, a giant Japanese retailer fell prey to a major attack where "more than 460,000 online customer accounts were fraudulently accessed between April 23 and May 10, 2019. Personal information that may have been exposed in the attack includes first and last names, full residential and shipping addresses, landline and mobile phone numbers, email address, gender, date of birth, purchase history, and partial credit card information including cardholder, expiration date, and part of credit card number." *See* "Security breach hits apparel giant," May 14, 2019.

Unfortunately, many users unwittingly facilitate these attacks by repurposing their easily cracked passwords for multiple accounts.

## What Are Credential Stuffing Attacks?

Hundreds of millions of email addresses and passwords sit on the dark web. Some are purchased and quickly used, while some are held and accumulated for further criminal use at a later date. In a credential stuffing attack, attackers use previously stolen addresses and passwords (called "credentials"), coupled with advanced, automated tools to attempt millions of log-ins to a customer- or consumer-facing website. Even if most attempts are thwarted, with millions of attempts, some are bound to succeed, allowing hackers to monetize their investments. According to an April 25 article (referencing a February 2019 report),

> 'with an investment of as little as $550, criminals could expect to earn at least 20 times the profit on the sale of compromised login credentials.' [] For the $550, the crooks can get a $150 checking software, a leaked/stolen credentials database of roughly 100K user records, and enough proxies to run their credential attacks for $250/week….[The report notes] that 'for every one million random combinations of emails and passwords, attackers can potentially compromise between 10,000 and 30,000 accounts. Moreover, the same database could then be reused over and over again to hack dozens of different websites, yielding even higher profits.'

*See* "The Anatomy of Highly Profitable Credential Stuffing Attacks."

The relatively small investment necessary to commence one of these infiltrations is demonstrated by the large numbers of attempted credential stuffing attacks. Indeed, the report "showed that approximately 28 billion credential stuffing attempts were detected between May and December 2018, retail websites being the main targets of credential abuse with 10 billion attempts." (*see* "Credential Abuse per Day" chart in above-linked article).

## What Can You Do About Credential Stuffing Attacks?

Given that databases are being left open to theft in the wild Internet ecosystem, these attacks will likely continue at a rapid pace, especially for retailers with customer-facing websites available for log in. To minimize the likelihood of a credential stuffing attack and the resultant damage, your company may wish to consider the following basic potential safeguards:

1. Use multi-factor or two-factor authentication, requiring the person signing in to spend an additional step to insert a code sent back to him or her (generally by text message).

2. Check your logs to see if there are massive, failed attempts to log in. That is a tell-tale sign that an attacker is trying what might be millions of different passwords or email addresses to log in.

3. In similar fashion, if there are multiple attempts to log in, you can limit login attempts to, for example, five per 15 minutes per IP address, or limit attempts to three, and then lock out that person/ID.

4. Use the "I am not a robot" defensive tool called "Captcha." Although requiring customers to select traffic light or storefront images may seem cumbersome, it can frustrate a credential stuffing attack.

5. Implement a mandatory password reset if your company discovers its customers' credentials have been stolen.

With millions of customers and accounts, retailers are a regular target for credential stuffing attacks. While the defensive measures retailers need to take to secure their networks seem endless, the safeguards to protect against a successful credential stuffing attack noted above are relatively easy to implement, and much easier than handling a data breach involving millions of customers.

## Author

This GT Alert was prepared by **Paul Ferrillo**. Questions about this information can be directed to:

- Paul Ferrillo | +1 212.801.6598 | ferrillop@gtlaw.com
- Ian C. Ballon | +1 650.289.7881 | ballon@gtlaw.com
- Dr. Viola Bensinger | +49 30.700.171.150 | viola.bensinger@gtlaw.com
- Kate Black | +1 415.655.1300 | blackk@gtlaw.com
- Lori Chang | +1 310.586.3863 | changl@gtlaw.com
- Francoise Gilbert | +1 650.804.1235 | gilbertf@gtlaw.com
- David M. Greenberg | +1 212.801.6545 | greenbergdm@gtlaw.com
- Carsten Kociok | +49 30.700.171.119 | carsten.kociok@gtlaw.com
- Carmina Mogollón González | +52 55.5029.0034 | mogollonc@gtlaw.com
- Gretchen A. Ramos | +1 415.655.1319 | ramosg@gtlaw.com
- Radboud Ribbert | +31 (0) 20.301.7333 | ribbertr@gtlaw.com
- Alan N. Sutin | +1 212.801.9286 | sutina@gtlaw.com
- Hans Urlus | +31 (0) 20.301.7324 | urlush@gtlaw.com
- Or your Greenberg Traurig attorney

Albany. Amsterdam. Atlanta. Austin. Boca Raton. Boston. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Germany.¬ Houston. Las Vegas. London.* Los Angeles. Mexico City.+ Miami. Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Sacramento. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. ¬Greenberg Traurig's Berlin office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. *Operates as a separate UK registered legal entity. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. ¤Greenberg Traurig Tokyo Law Offices are operated by GT Tokyo Horitsu Jimusho, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by Greenberg Traurig Grzesiak sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in Greenberg Traurig Grzesiak sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2019 Greenberg Traurig, LLP. All rights reserved.*