RSA BUSINESS-DRIVEN SECURITY™

RSA QUARTERLY FRAUD REPORT

Volume 3, Issue 1
Q1 2020

CONTENTS

EXECUTIVE SUMMARY

The RSA® Quarterly Fraud Report presents an analysis of fraud attack and consumer fraud data collected by the RSA Fraud and Risk Intelligence team in the course of its work identifying threats for RSA customers. As such, it provides a glimpse into the cyber fraud landscape for consumer-facing organizations of all sizes and types.

RSA-OBSERVED FRAUD ATTACK AND CONSUMER TRENDS

For the period starting January 1, 2020, and ending March 31, 2020, RSA observed several global fraud trends across attack vectors and digital channels. The highlights include:

In Q1 2020, RSA identified a total of 50,119 global fraud attacks.

Phishing remains the predominant attack vector used by fraudsters, accounting for 54% of all cyber attacks observed by RSA in Q1.

Brand abuse attacks in Q1 were up 12% over the previous quarter, and constituted 22% of total attacks in Q1, an increase of 5 percentage points over the previous quarter.

For the fifth quarter in a row, Canada was by far the most frequently targeted country for phishing, with 66% of all attacks. (The next most frequently targeted accounted for only 7%.)

The percentage of fraud transactions originating from a mobile app doubled in Q1 to 26%, from 13% in Q4 2019.

In online banking payments, the percentage of transaction volume from new accounts doubled.

FEATURE ARTICLE

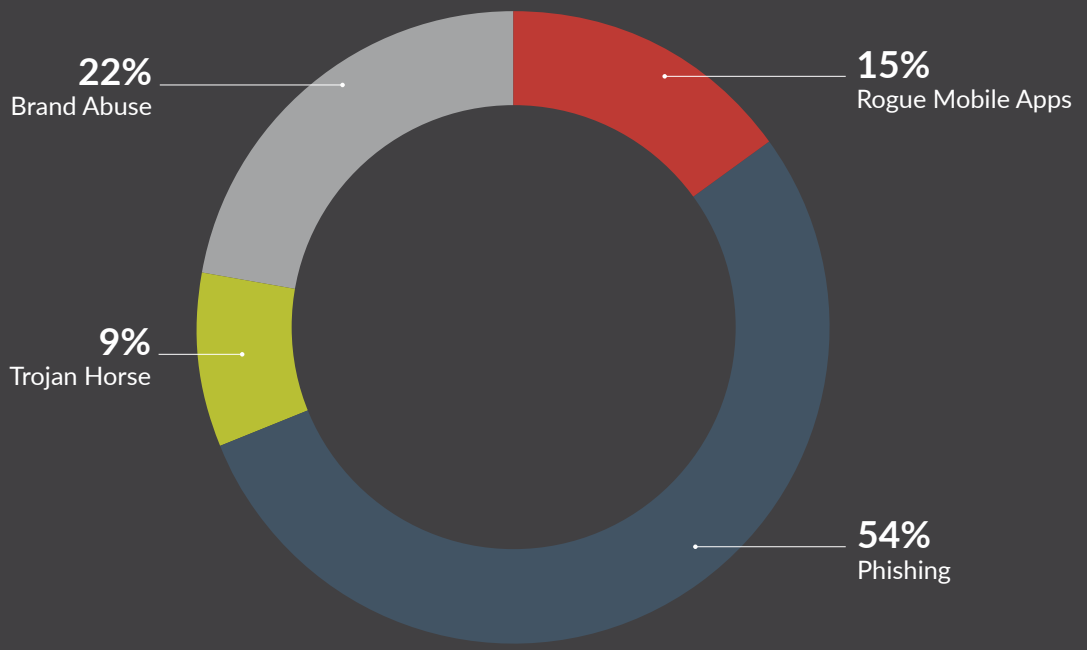
The Rapid Rise of COVID-19 Fraud

Fraudsters are always eager to exploit consumers' vulnerabilities, and they have been quick to take advantage of the fear and uncertainty surrounding COVID-19. From phishing emails that lure people into clicking through for health safety information, to social media ads promising free goods or services at a time of financial insecurity, there has been no shortage of scams designed to strike at COVID-19 concerns. In this article, we share information about a variety of types of pandemic-specific fraud observed by RSA analysts during Q1.

FRAUD ATTACK TRENDS: Q1 2020

Phishing and malware-based attacks are the most prolific online fraud tactics developed over the past decade. Phishing attacks not only enable online financial fraud, but these sneaky threats also chip away at our sense of security as they get better at mimicking legitimate links, messages, accounts, individuals and sites. Automated fraud comes in the form of the various active banking Trojan horse malware families in the wild today; these malicious programs do their work quietly and often without detection until it is too late.

By tracking and reporting the volume and regional distribution of these fraud threats, RSA hopes to contribute to the ongoing work of making consumers and organizations more aware of the current state of cybercrime and fueling the conversation about combating it more effectively.



Fraud Attack Trends: Q1 2020

Fraud Attack Type Distribution

In the first quarter of 2020, RSA identified 50,119 cyber attacks worldwide. The greatest percentage of these were phishing attacks, representing 54% of all attacks identified. The next greatest percentage was brand abuse, which made up 22% of all attacks (an increase of 5 percentage points over the previous quarter). The high volume of brand abuse attacks can be attributed to the growing trend of fraudsters luring in victims with fake domains that resemble legitimate websites. This trend has also been popular in COVID-19-related scams, as described in this quarter's feature article on page 13.

FRAUD ATTACK GLOSSARY

Phishing
Cyber attacks attempting to steal personal information from unwitting end-users under false pretenses either by email, phone call (vishing) or SMS text (smishing).

Trojan Horse
Stealthy malware installed under false pretenses, attempting to steal personal user information.

Brand Abuse
Online content, such as social media, that misuses an organization's brand with the purpose of misleading users.

Mobile Application Fraud
Mobile applications using an organization's brand without permission.

IN Q1 2020,

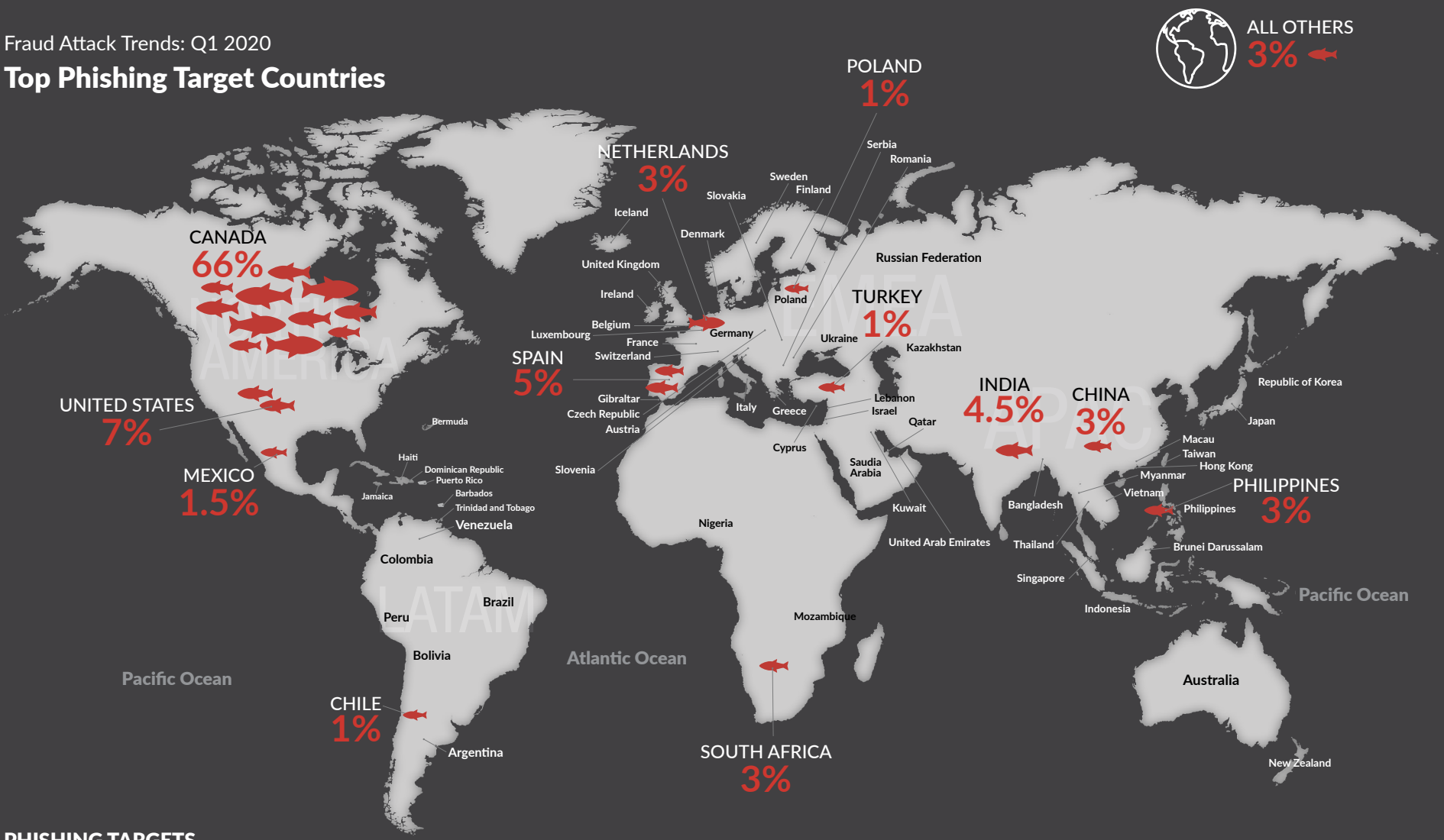
27,054

ATTACKS WERE THE RESULT OF PHISHING

8% more than all other attack types combined

Fraud Attack Trends: Q1 2020

Top Phishing Target Countries



PHISHING TARGETS

Canada continues to dominate the list of top targeted countries for phishing attacks. The country was the target of 7 out of 10 phishing attacks for the second year in a row, making it the top targeted country for every quarter of the last four. The United States was again second on the list. Most of the countries in the top 10 saw a decrease in total attacks, except for China (up 67.5%), South Africa (up 72%) and the Philippines (up 30%).

Top Phishing Hosting Countries

HOSTING COUNTRIES

1.	United States	6.	Malaysia
2.	China	7.	Canada
3.	Germany	8.	France
4.	India	9.	Hong Kong
5.	Russia	10.	United Kingdom

PHISHING HOSTS

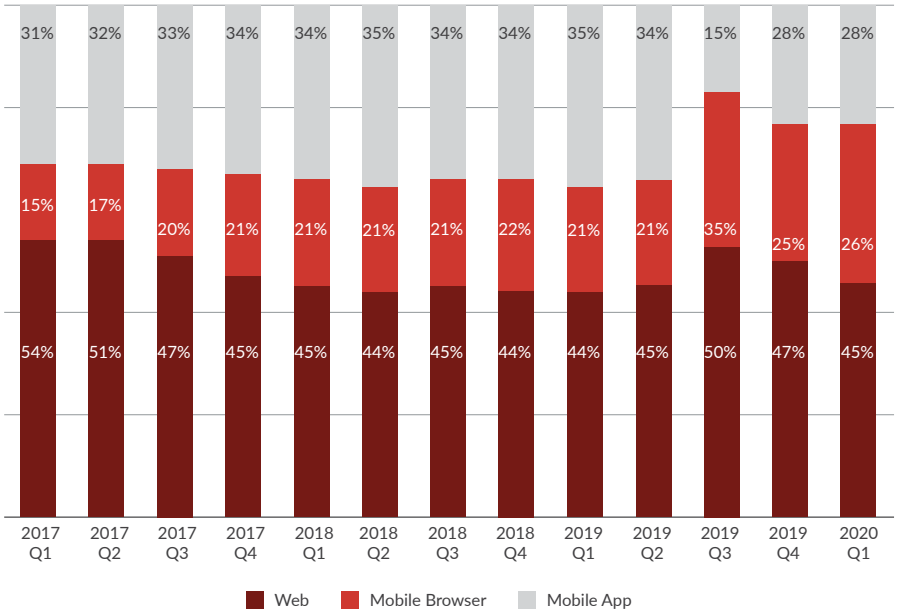
The United States continues to be the top hosting country for phishing attacks, accounting for almost 60% of ISPs hosting these types of attacks. This is largely attributable to a handful of large-scale hosting authorities, whose sheer magnitude makes it easy for fraudulent activity to go undetected.

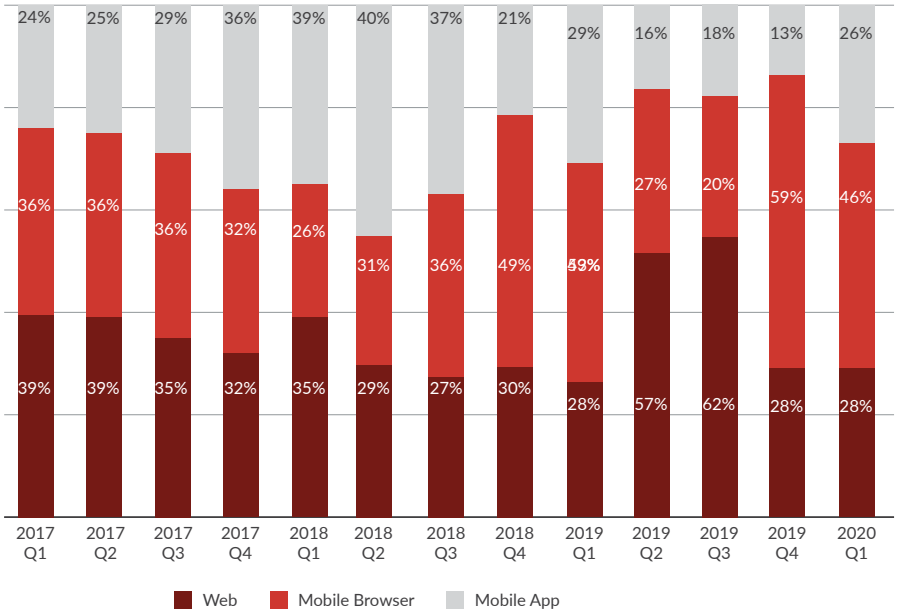
CONSUMER FRAUD TRENDS: Q1 2020

The RSA Fraud and Risk Intelligence team analyzes consumer fraud data and informs the security and risk management decisions for major organizations while serving the public interest by identifying, preventing and reducing financial cyber fraud attacks on consumers. Observing consumer fraud trends over time can support decision-makers on how to build or refine their digital risk management strategy across customer-facing digital channels.

These data points are intended to broadly frame the current consumer fraud atmosphere, and identify relevant trends, by tracking broad indicators of online fraud across both financial and e-commerce focus areas.

Transaction and Fraud Transaction Distribution by Channel





Source: RSA Fraud & Risk Intelligence Service, January 2020-March 2020

TRANSACTION METHOD

In the first quarter of 2020, mobile browsers and mobile applications accounted for 54% of overall transactions observed by RSA, reflecting very little change from the previous quarter.

26% of fraud transactions originated from a mobile app, double the percentage in the previous quarter

FRAUD TRANSACTION METHOD

While the overall volume of fraud originating on the web vs. the mobile channel in Q1 2020 was essentially unchanged from the previous quarter, the distribution within the mobile channel changed significantly. Q1 2020 was remarkable for the jump in the volume of fraud transactions originating in a mobile app, rather than a mobile browser; it doubled from 13% in Q4 2019 to 26% in Q1 2020. This is the highest percentage of fraud transactions originating from a mobile app observed by RSA since Q2 2018. There was a corresponding decrease of 13% in fraud transactions originating from a mobile browser, while those originating from the web held steady at 28%, underscoring the idea of a shift from mobile browser to mobile app as a source of fraud, rather than a move from the web to the mobile channel overall.

Average Credit Card Transaction and Fraud Transaction Values

(E-Commerce, by Region)

In Q1 2020, the greatest average fraud transaction value was $364, in Australia and New Zealand, which is 26% higher than the next nearest amount of $269 in the EU. Australia and New Zealand also had the greatest difference between the value of genuine and fraudulent credit-card transactions, with the average fraud transaction value at nearly triple the value of a genuine transaction. (That is less of a difference in value than in the previous quarter, but it remains the highest difference of all the regions.) Also noteworthy is that across all regions, average transaction values changed very little this quarter; however, fraud transaction values went up in the EU, down in the Americas and Australia/New Zealand, and saw little change in the UK. Notably, the average value of a fraudulent payment transaction in the mobile channel increased by 60% in Q1, from $480 to $767.

REGION	TRANSACTION VALUE	FRAUD TRANSACTION VALUE	DIFFERENCE $
European Union	$134	$269	$135
Americas	$213	$218	$5
UK	$175	$249	$74
Australia/New Zealand	$134	$364	$230

Source: RSA Fraud & Risk Intelligence Service, January 2020-March 2020

Device Age vs. Account Age

ANALYSIS

"Device Age" refers to how long the RSA Fraud Platform has "known" or "trusted" a given device (laptop, smartphone, etc.). "Account Age" refers to how long the RSA Fraud Platform has "known" or "trusted" a given account (login, etc.). This data demonstrates the importance of accurate device identification to minimize false positives and customer friction during a login or transaction event.

E-COMMERCE

In Q1 2020, 58% of fraud transaction value originated from a new device but trusted account. This reflects little change from the previous quarter, indicating that account takeover activity continues to be a preferred attack vector.

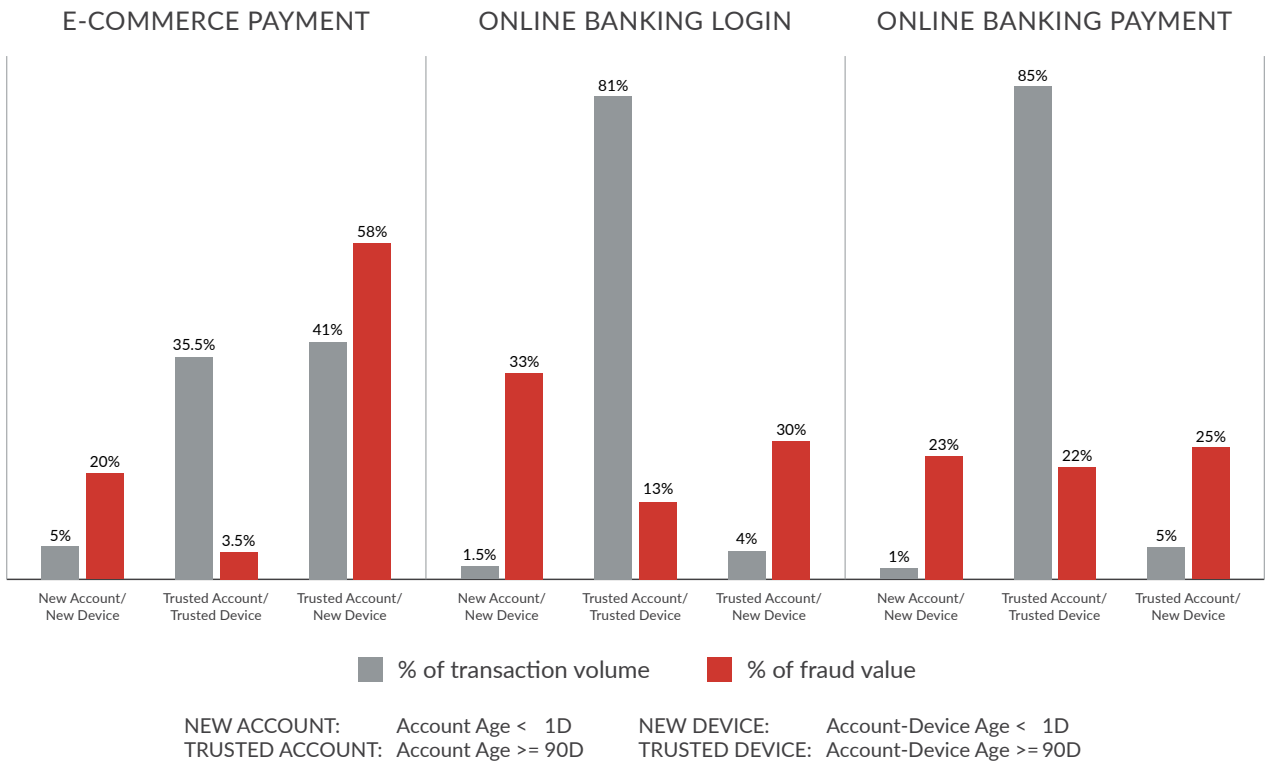
ONLINE BANKING: LOGIN

While only 1.5% of logins were attempted from a combination of new account and new device, this scenario accounted for 33% of total fraud volume observed in Q1. This is down from 41% the previous quarter, but is still a significant gap, which suggests fraudsters are continuing to use stolen credentials from data breaches to set up mule accounts to facilitate cash out or new account fraud, albeit at a lower rate.

ONLINE BANKING: PAYMENT

In Q1, only 1% of total payment transactions came from a new account and a new device, but 23% of fraud value was in this category. In addition, the percentage of fraud value associated with a combination of trusted account and trusted device was 22%, up 7% over the previous quarter.

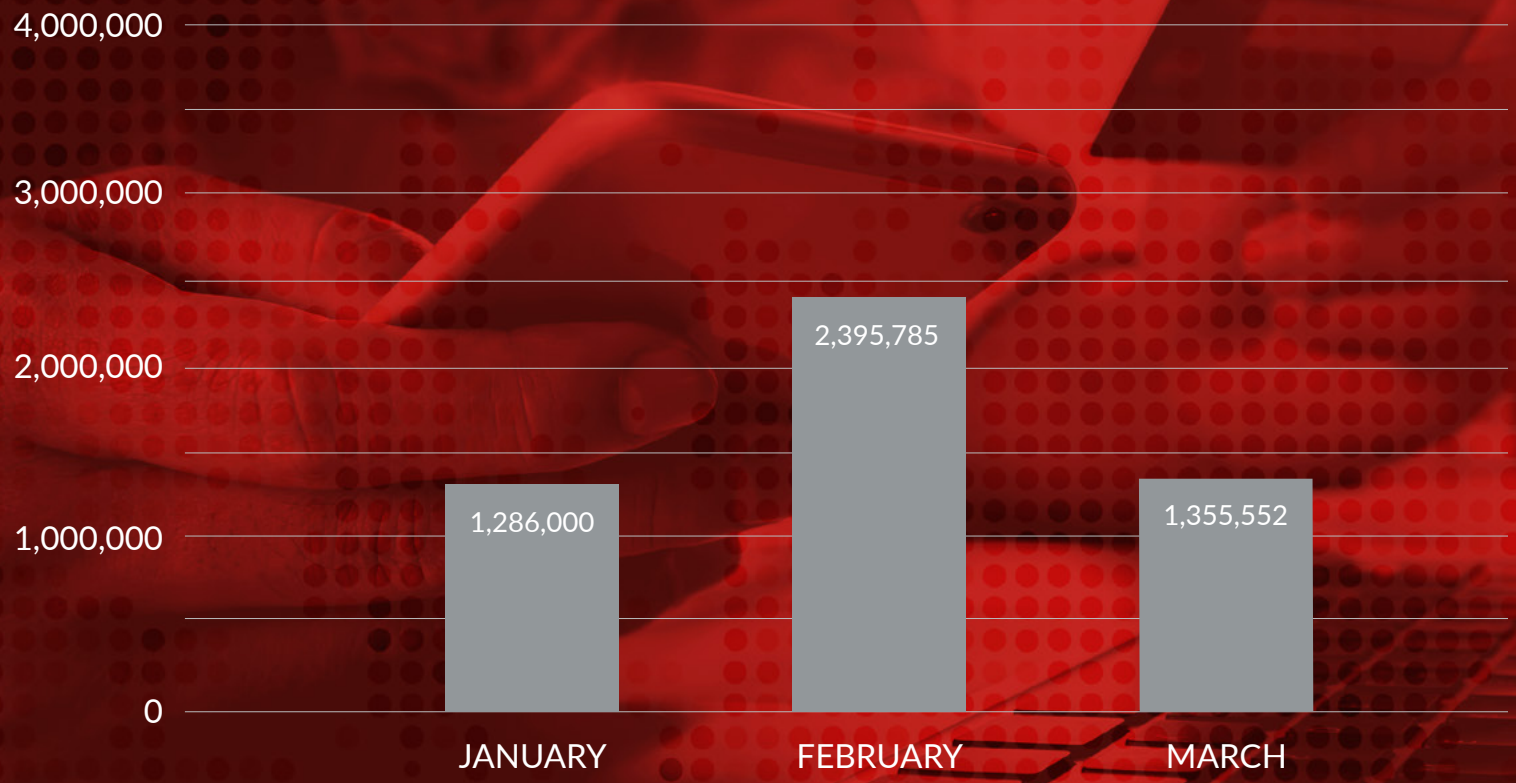
One interesting development this quarter is that while the total percentage of new accounts being used for online banking logins and payments is still relatively low, at 1.5%, that figure is triple the .5% reported in Q4 2019. This tracks with a recent RSA Fraud and Risk Intelligence analysis indicating a notable increase in new investment accounts in February and March 2020, which may be the result of investors looking for a safe place to put their money when stocks were dropping because of COVID-19.



NEW ACCOUNT: Account Age < 1D
TRUSTED ACCOUNT: Account Age >= 90D
NEW DEVICE: Account-Device Age < 1D
TRUSTED DEVICE: Account-Device Age >= 90D

Source: RSA Fraud & Risk Intelligence Service, January 2020-March 2020

Compromised Credit Cards Discovered/Recovered by RSA



Source: RSA Fraud & Risk Intelligence Service, January 2020-March 2020

ANALYSIS

In Q1 2020, RSA recovered over 5 million unique compromised cards and card previews from online credit card stores and fraud communication channels. Fraudsters categorize compromised cards as “CVV2” or “dumps,” depending on how they were compromised; RSA FraudAction™ service collects CVV2-related data, which is card data compromised through cyber attacks targeting online transactions or e-commerce. This type of compromised card data can be used for a variety of fraudulent activities, including “carding,” which refers to using compromised cards to buy goods both in physical stores and on e-commerce websites.

FEATURE ARTICLE

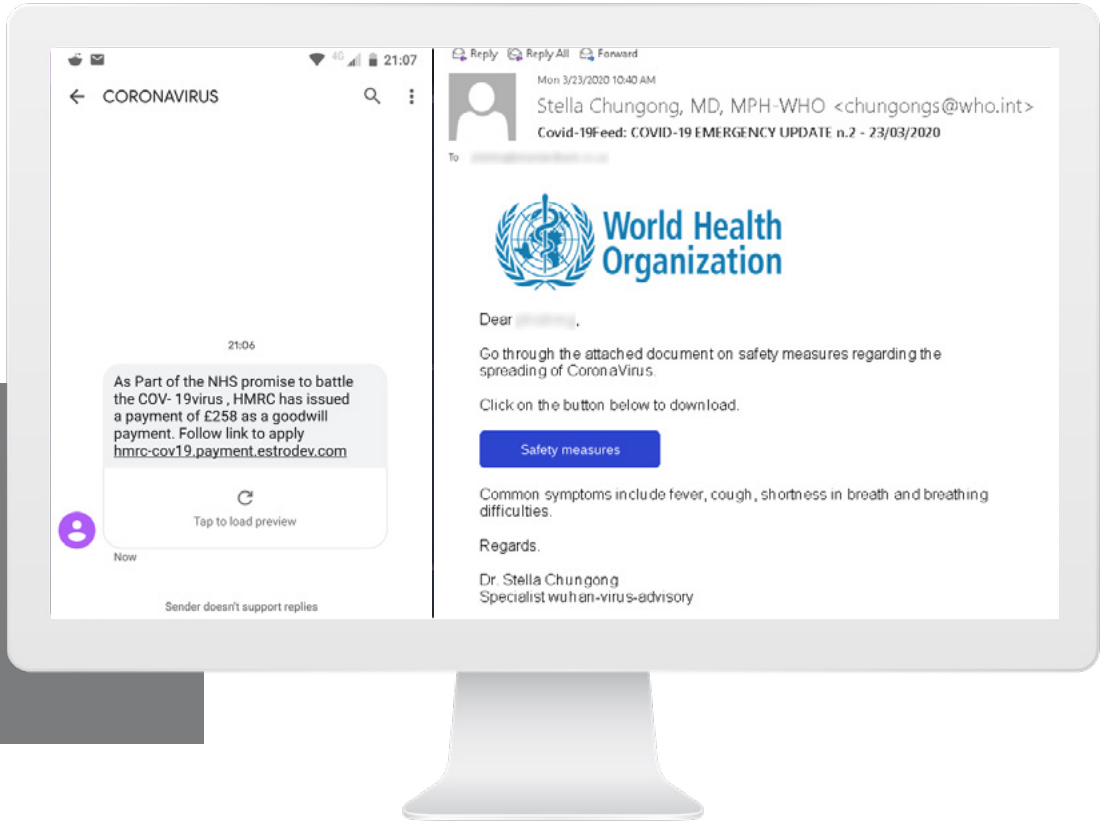
The Rapid Rise of COVID-19 Fraud

The current global health crisis has had many surprising consequences, from frightening shortages of supplies for healthcare personnel to welcome decreases in air, water and noise pollution from a variety of sources. But one effect that should come as no surprise to anyone is the surge in cybercrime that has accompanied the crisis. After all, past experience has demonstrated that anytime there is an event that causes fear or insecurity, cybercriminals will be quick to exploit it. When a natural disaster strikes, scam emails and texts targeting everyone from victims to potential donors follow in its wake. Even predictable events, like the tax filing season or the holiday season, are invariably accompanied by scams. In this article, we take a closer look at some of the different types of scams RSA has seen in light of COVID-19, the impact on consumers and health organizations, and what can be done to fight back against those who are exploiting the ongoing crisis.

In this article, we take a closer look at some of the different types of scams RSA has seen in light of COVID-19, the impact on consumers and health organizations, and what can be done to fight back.

Phishing, Brand Abuse and More—Now with a COVID-19 Twist

While the cyber attacks used to harvest data have not changed as a result of COVID-19, they have definitely taken on a new shape and form. The U.S. Federal Trade Commission[1] has warned consumers to be on the lookout for phishing emails and texts that prey on financial insecurities by dangling promises of relief payments and cash grants, or that target health fears by offering to share information on how to avoid infection with the virus. Here are just a couple of examples of COVID-19-related scams RSA FraudAction researchers identified, in which a text or email purports to come from a trusted source:



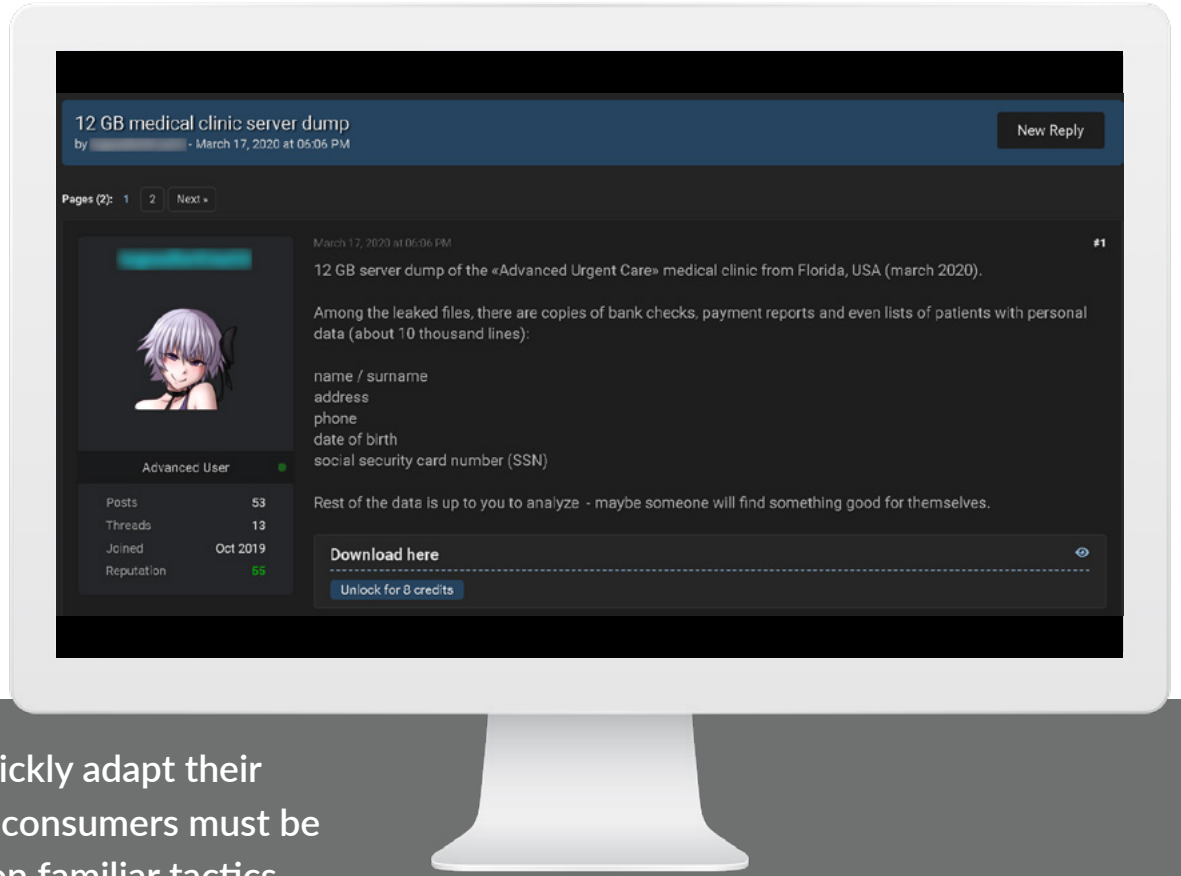
You can learn more about these and other COVID-19 scams, and see additional examples of nefarious activity (including cybercriminal communications in underground forums, as well as in plain sight on social media) in the RSA FraudAction Intelligence Threat Report, The Cybercrime Landscape Amid COVID-19.[2]

It bears remembering that because fraudsters are known to quickly adapt their behavior based on changing events, consumers must be continually alert for new variations on familiar tactics. For example, once contact tracing became a prominent news topic, phishing and other scams quickly materialized to prey on consumer fears of being infected. A recent consumer notice from the Federal Trade Commission warned of text messages[3] telling recipients someone they had been in contact with had tested positive for COVID-19 and asking them to—you guessed it—click on a link to learn more.

Medical Testing Facilities and Other Health Organizations Become Targets

Consumers aren't the only ones targeted for COVID-19-related cybercrime. Just days after cyber attackers made a public vow not to victimize health and medical organizations[4] during the pandemic, a medical facility preparing to test coronavirus vaccines was hit by a ransomware attack from one of the very groups that had made the promise not to do it. The attackers gained access to thousands of patient records[5] and attempted to hold them for ransom—but the facility was fortunately able to restore the information without paying the ransom. (Still, some of the information in the records was leaked online.) Within a few weeks of that particular attack, Interpol issued a global warning[6] about the threat of ransomware attacks on hospitals.

In the example below, an online "leak forum" offers cybercriminals access to leaked patient files from a medical clinic. RSA FraudAction researchers traced this breach, which uncovered not just patients' medical records but also high-value PII, SSNs and banking records.



Because fraudsters are known to quickly adapt their behavior based on changing events, consumers must be continually alert for new variations on familiar tactics.

Fighting Back Against COVID-19 Fraud

Whether the targets are consumers or organizations, the keys to avoid being victimized are the same: awareness and preparation. Organizations like WHO, the Federal Trade Commission, Interpol and others are all using their websites to get the word out about the types of scams and attacks that are occurring and how to protect against them.

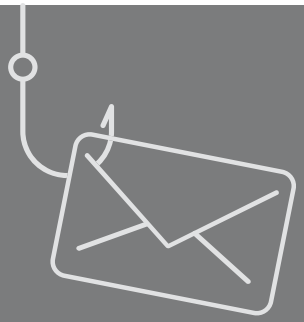
For consumers, being safe from scams means being alert for scam emails, texts and social media posts and messages, and knowing the tell-tale signs to look for, both in the nature of the communication (claiming there's a problem or offering money or other rewards, for example) and in the nature of the request they make (such as asking the recipient to click on a link or provide personal data).

For health facilities and other organizations whose risk of cyber attack and fraud has increased with COVID-19, the same guidance applies as for any organization seeking to mitigate the risk:

- Secure mail systems with strong spam filters are vital to preventing employees from being targeted.
- Keeping all hardware and software up to date, including regularly installing software patches, is critical to protect against cyber attacks.
- Because ransomware in particular relies on holding critical information for ransom, organizations will also benefit from regularly backing up that kind of data and storing backups in a different location.

Looking at risk in a larger context, many organizations responded to the pandemic early on by encouraging consumers to interact and transact with them in digital channels whenever possible, to reduce contact-related risk. But such policies inevitably increase digital risk. Organizations would therefore be well-advised now to take steps to assess their omnichannel fraud prevention strategy, explore cross-channel vulnerabilities and ensure that fraud prevention tools align with strategy.

Whether the targets are consumers or organizations, the keys to avoid being victimized are the same: awareness and preparation.



In conclusion, the idea of cybercriminals taking advantage of a life-threatening pandemic for financial gain is repellent, and its constantly changing nature and global reach can make it tough to combat. But both public and private entities are working hard against it, and there is also much that individuals and organizations, armed with information and awareness, can do to avoid being victims.

1 Cristina Miranda, "**Scammers are using COVID-19 messages to scam people**," U.S. Federal Trade Commission, Consumer Information, April 10, 2020

2 RSA Link, **RSA FraudAction Report: The Cybercrime Landscape amid COVID-19**, April 7, 2020

3 Colleen Tressler, "**COVID-19 contact tracing text message scams**," U.S. Federal Trade Commission, Consumer Information, May 19, 2020

4 Davey Winder, "**Hackers Promise 'No More Healthcare Cyber Attacks' During COVID-19 Crisis**," Forbes, March 19, 2020

5 Nathan Eddy, "**WHO, coronavirus testing lab hit by hackers as opportunistic attacks ramp up**," Healthcare IT News, March 24, 2020

6 "**Cybercriminals targeting critical healthcare institutions with ransomware**," Interpol, April 4, 2020

DIGITAL RISK IS EVERYONE'S BUSINESS
HELPING YOU MANAGE IT IS OURS

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk digital world at rsa.com

RSA