RSA BUSINESS-DRIVEN SECURITY™

RSA QUARTERLY FRAUD REPORT

Volume 1, Issue 2
Q2 2018

CONTENTS

EXECUTIVE SUMMARY

The RSA® Quarterly Fraud Report contains fraud attack and consumer fraud data and analysis from the RSA Fraud & Risk Intelligence team. It represents a snapshot of the cyber-fraud environment, providing actionable intelligence to consumer-facing organizations of all sizes and types to enable more effective digital risk management.

RSA-OBSERVED FRAUD ATTACK AND CONSUMER TRENDS

For the period starting April 1, 2018, and ending June 30, 2018, RSA observed several global fraud trends across attack vectors and digital channels. The highlights include:

Phishing accounted for 41 percent of all fraud attacks observed by RSA in Q2. Canada, the United States and the Netherlands were the top three countries most targeted by phishing.

RSA detected 9,185 rogue apps, which accounted for 28 percent of all fraud attacks.

Fraud from mobile browsers and mobile applications increased in Q2 2018 and represented 71 percent of total fraud transactions.

While less than one-half of one percent of legitimate payment transactions were attempted from a new account and new device, this combination accounted for 27 percent of the total value of fraudulent payments.

FEATURE ARTICLE

The "Human-Not-Present" World

With global industry pouring money, attention and effort into relatively new technologies such as artificial intelligence (AI), machine learning and the Internet of Things (IoT), it is clear that we're currently living in the early stages of what has the potential to be a profoundly technology-driven future. Responsible minds among the identity assurance and anti-fraud set have begun to see a familiar theme emerging in business and technology. The modern techno-philosophy seems to be moving rapidly toward increased frequency and depth of automation directed toward tasks that traditionally required human participation, thus giving rise to a new age, one consisting of "Human-Not-Present" transactions. This article explores the evolution of payments—from cash-present to human-not-present—including the role of identity in all transactions and the potential security gaps it leaves.

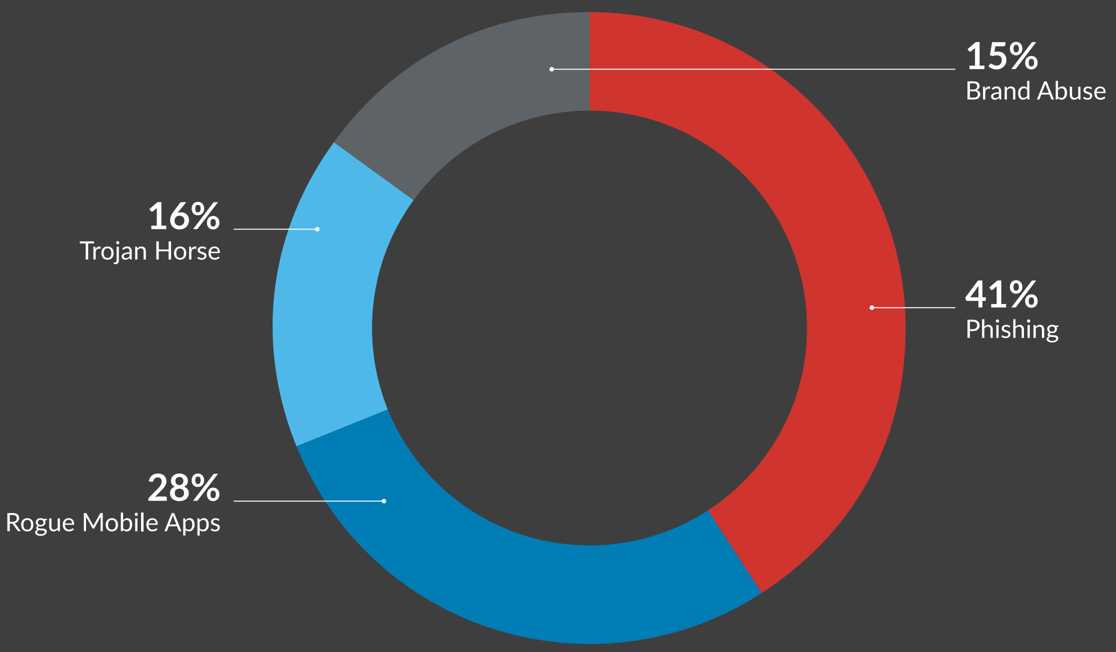
FRAUD ATTACK TRENDS: Q2 2018

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: Q2 2018

Fraud Attack Type Distribution



In the second quarter of 2018, phishing attacks accounted for 41 percent of all observed fraud attacks, a slight decrease from 48 percent last quarter. Attacks involving financial malware dropped from 25 percent last quarter to 16 percent in Q2. RSA detected 9,185 rogue mobile applications, representing a 13 percent increase from last quarter and 28 percent of observed attacks.

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 Q2 2018,
RSA identified
9,185
ROGUE MOBILE
APPLICATIONS

Fraud Attack Trends: Q2 2018

Top Phishing Target and Hosting Countries

TARGET COUNTRIES

1.	Canada	🇨🇦
2.	United States	🇺🇸
3.	Netherlands	🇳🇱
4.	India	🇮🇳
5.	Spain	🇪🇸
6.	Brazil	🇧🇷
7.	Colombia	🇨🇴
8.	France	🇫🇷
9.	Peru	🇵🇪
10.	Mexico	🇲🇽

HOSTING COUNTRIES

1.	United States	🇺🇸
2.	India	🇮🇳
3.	Canada	🇨🇦
4.	Russia	🇷🇺
5.	Germany	🇩🇪
6.	Netherlands	🇳🇱
7.	Australia	🇦🇺
8.	Malaysia	🇲🇾
9.	Italy	🇮🇹
10.	France	🇫🇷

PHISHING TARGETS

The Netherlands and Spain saw an increase in phishing attacks in Q2, driving both into the top five most targeted countries. France is a new entrant to the Top 10 Target list this quarter, while we saw South Africa drop off. Not surprisingly, Canada and the United States remain the two countries most targeted by phishing.

PHISHING HOSTS

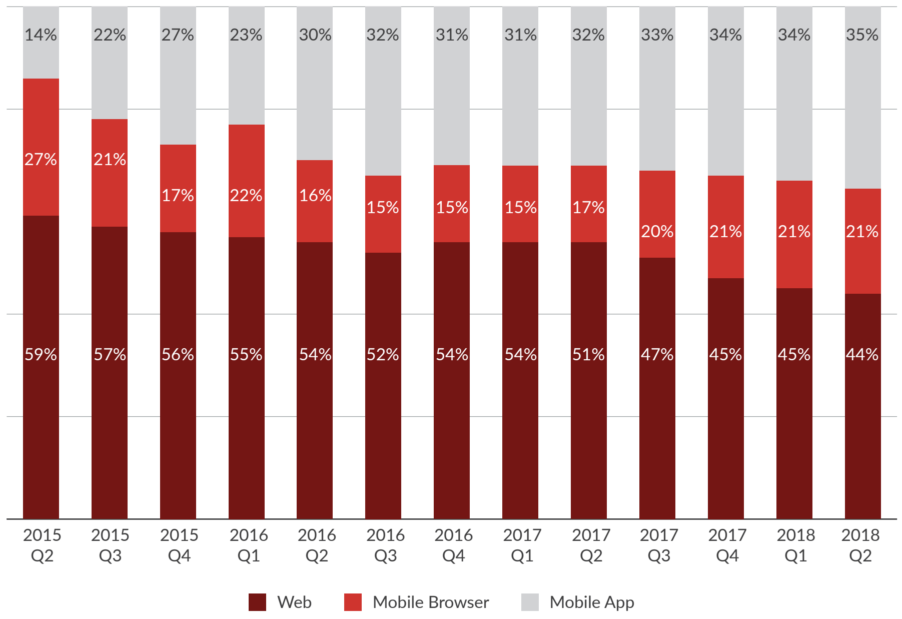
There were some interesting changes in the top hosting countries quarter over quarter. In Q2, new entrants to the list include the Netherlands, Australia, and Malaysia. There was a slight decrease in the number of attacks hosted in Russia, while we saw China and Luxembourg fall off the list this quarter.

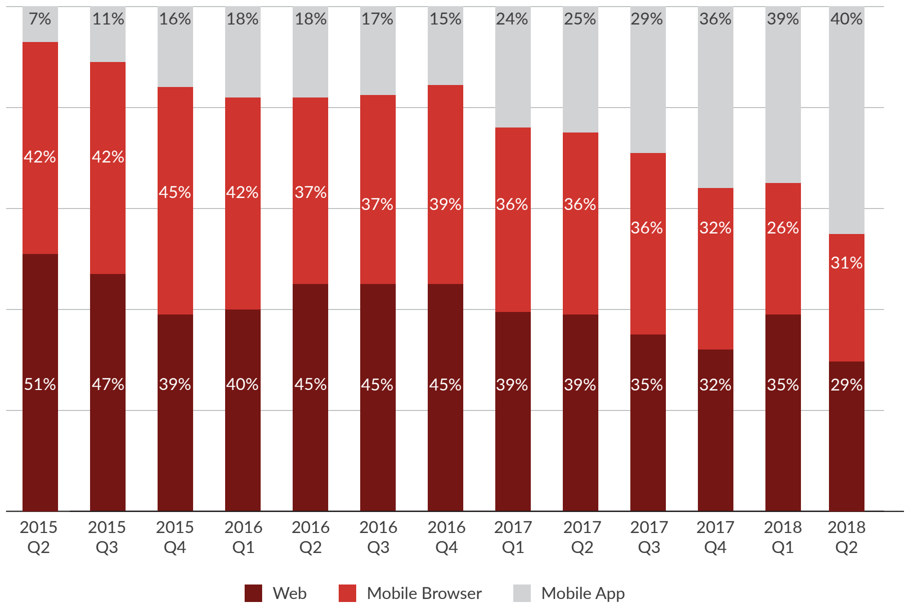
CONSUMER FRAUD TRENDS: Q2 2018

Quantifying cyber fraud is no simple task. Even with a deep data set, few organizations have the necessary depth of insight into the anti-fraud landscape to understand the nuance involved in tracking people and tactics that are specifically trying to remain hidden. The RSA Fraud & 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.

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, April 2015-June 2018

TRANSACTION METHOD

In the second quarter of 2018, mobile browsers and applications accounted for 56 percent of legitimate transactions observed by RSA, representing little change in channel distribution from the previous quarter. Year over year, however, overall mobile use for legitimate transactions has risen 14 percent.

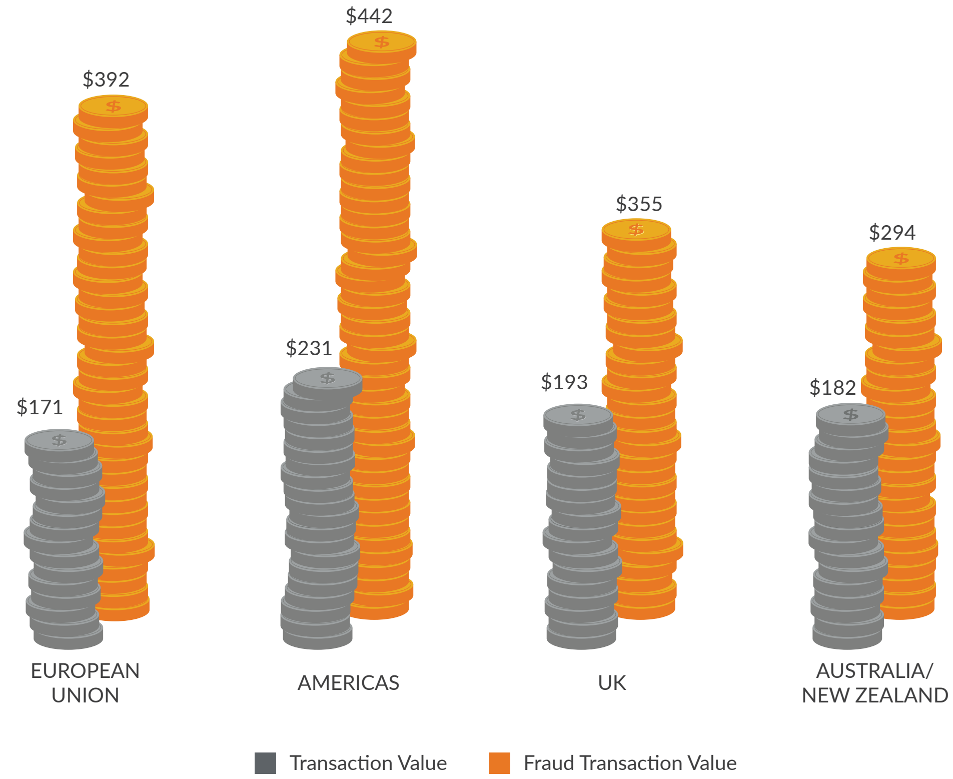
FRAUD TRANSACTION METHOD

In Q2, mobile application and mobile browser transactions made up 71 percent of overall fraud transactions, a 9 percent increase from Q1 2018. Year over year, fraud transactions by mobile applications and browsers have increased 16 percent.

Consumer Fraud Trends: Q2 2018

Average Credit Card Transaction and Fraud Transaction Values

(E-Commerce, by Region)



The average value of a fraudulent transaction will likely always be higher than that of a genuine transaction, since fraudsters regularly use stolen credit cards to make quick, high-value purchases because these goods are easy to resell for a profit. There are, however, insights to be gained in the differences between the spending levels related to genuine and fraud transactions.

In the first quarter, the most drastic difference between the value of genuine and fraud transactions was observed in Europe (minus the U.K.), where the average value of a fraudulent transaction was $392, a 78 percent difference than the average genuine transaction. The Americas (including U.S. and Canada) observed a 13 percent decrease in the average fraud transaction value, declining from $508 in Q1 to $442 this quarter.

REGION	TRANSACTION VALUE	FRAUD TRANSACTION VALUE	DIFFERENCE $	DIFFERENCE %
European Union	$171	$392	$221	+79%
Americas	$231	$442	$211	+63%
UK	$193	$355	$162	+59%
Australia/New Zealand	$182	$294	$112	+47%

Source: RSA Fraud & Risk Intelligence Service, April 2018-June 2018

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

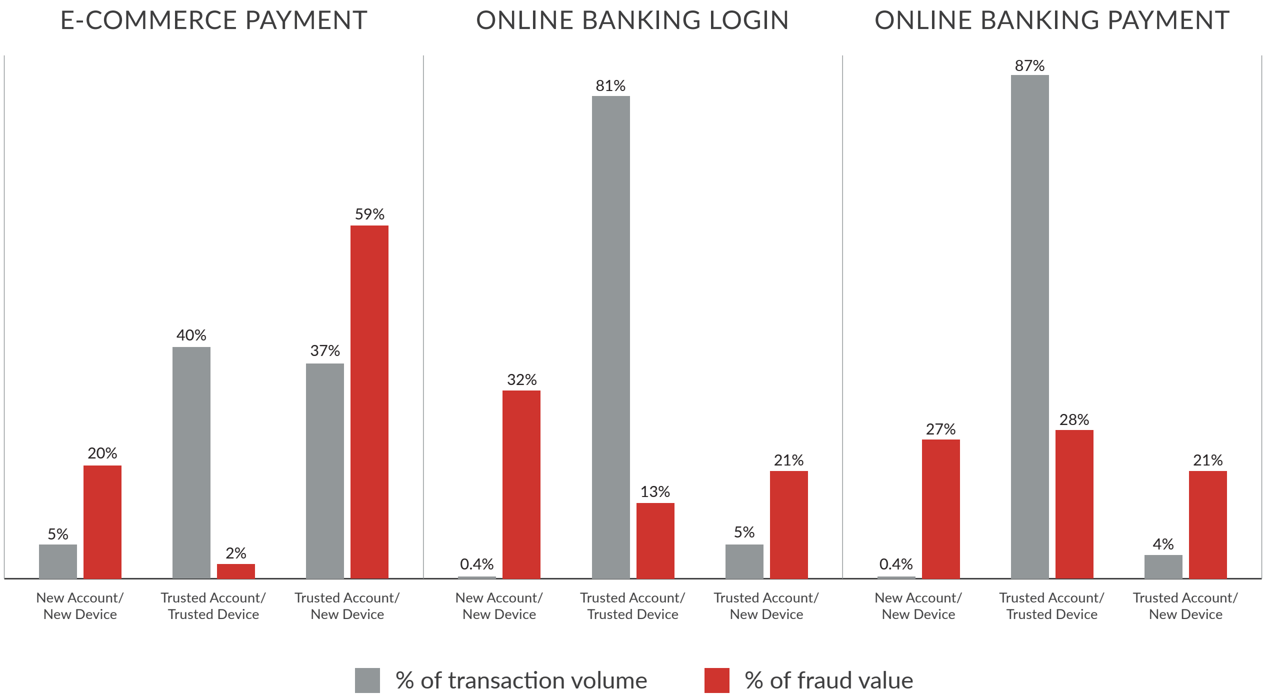
In the second quarter, 80 percent of fraud among e-commerce transactions originated from a new device. In the case of known/trusted accounts, 59 percent of fraud transaction value was from a new device, which is indicative of account takeover or password-guessing attacks where fraudsters could be attempting transactions from the same account across multiple merchants.

ONLINE BANKING: LOGIN

While less than half of a percent (0.4) of legitimate logins were attempted from a combination of a new account and new device, this scenario accounted for 32 percent of total fraud volume observed in Q2. This same pattern was also witnessed in Q1 and indicates fraudsters attempting to leverage stolen identities to create mule accounts as part of the “cash-out” process.

ONLINE BANKING: PAYMENT

Similar to fraud patterns at login, only 0.4 percent of legitimate payment transactions are attempted from a new account and new device, yet this combination makes up 27 percent of total fraud values, an increase from 22 percent last quarter. Twenty-eight percent of fraud originates from a known/trusted account and device, which suggests that there is a high likelihood of devices infected with financial malware capable of performing man-in-the-middle account takeover attacks.

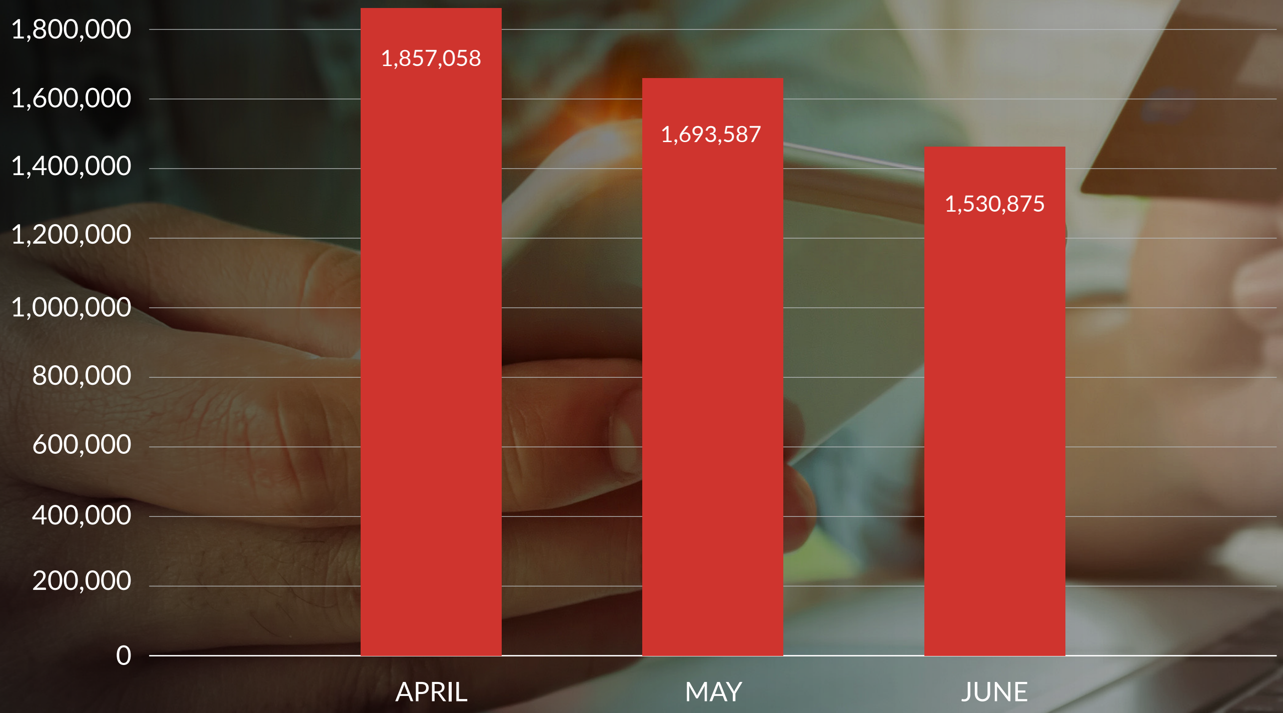


NEW ACCOUNT:	Account Age < 1D	NEW DEVICE:	Account-Device Age < 1D
TRUSTED ACCOUNT:	Account Age >= 90D	TRUSTED DEVICE:	Account-Device Age >= 90D

Source: RSA Fraud & Risk Intelligence Service, April 2018-June 2018

Consumer Fraud Trends: Q2 2018

Compromised Credit Cards Discovered/Recovered by RSA



Source: RSA Fraud & Risk Intelligence Service, April 2018-June 2018

ANALYSIS

In Q2 2018, RSA recovered nearly 5.1 million unique compromised cards and card previews from reliable online fraud stores and other sources. This represents a 60 percent increase in cards recovered by RSA in the previous quarter. While many credit card stores share the same database, RSA only monitors one store per database to avoid duplicates. These figures represent recovered cards with unique card information that can be used for online fraud.

The "Human-Not-Present" World

THE MACHINES ARE COMING.

Built by and to serve humanity, and imbued with newfound self-awareness, the creations turn on their creators, ushering in a terrible technological apocalypse.

While we are likely several generations of poor decision-making away from such a science fiction scenario, we must admit that in such a fable, there must have been a starting point. There had to have been some early time where exploiting the possibilities and opportunities of revolutionary technology seemed a more significant use of our energies than addressing the concerns and risks, especially those related to the distant future implications of our decisions.

With global industry pouring money, attention and effort into relatively new technologies such as AI, machine learning and the IoT, it is clear that we're currently living in the early stages of what has the potential to be a profoundly technology-driven future. The effects are already being seen in our society, where AI assistants, smart televisions, and self-driving vehicles already listen, learn and even anticipate some of our more basic wishes and needs.

PRESENCE NOT REQUIRED

Financial transactions of all sorts are being increasingly automated in this way. The evolution of payment methods, for example, is largely the story of how technology has, over time, fundamentally altered a core requirement of any value-based transaction: presence; starting with the ancient invention of currency, which allowed governments to regulate their economies based on its amount of "treasure," and allowed holders of that treasure to avoid carrying it around in the age of literal highway robbery.

CASH-PRESENT

The early "Cash-Present" age must have been characterized by insecure, inconvenient, in-person encounters that could cost as much in logistics (transport, security, lodging, etc.) as the transaction itself. Identity likely wasn't much of a concern, except maybe to keep track of one's debtors. The alternative was likely based on a promise and lots of trust, and at a time in history when neither was worth much without some kind of collateral.

CASH-NOT-PRESENT

The advent of the check (which is likely almost as old as money itself) formalized the "promise" of payment against an understanding of wealth, essentially creating a new "Cash-Not-Present" scenario. This was a more convenient/physically secure option, as it took the valuables (meant for payment) out of the equation while still allowing easy access to buying power. The trust, verification and security required for this new payment concept to work properly, however, meant that identity quickly became a critical issue for the first time. New crimes were created as criminals found ways to take advantage of a fledgling system built more on the promise of convenience than security.

An advancement in "Cash-Not-Present" transactions came with the advent of the first universal credit card, which is understood to have been Diners' Club in 1950.[1] Essentially a durable, reusable check, the credit card was tied to a ledger of expenses and transactions against the vouched-for wealth of the carrier, a carryover function from its use in the "company stores" of the Depression era. The increased convenience of a durable check came with a price: if stolen, the card could be used repeatedly, versus a one-time check. As such, identity became even more critical, and fraudsters took advantage, first through mail-order fraud schemes and eventually online cybercrime with the introduction of internet banking and eventually online payment at the end of the 20th century.

CARD-NOT-PRESENT

The mass adoption of the World Wide Web in this similar timeframe opened up new avenues of both payment convenience and electronic validation of identity, to say nothing of new methods and schemes for defrauding the new system. Banks were some of the first to offer customers the option to spend directly from their bank accounts, using new encryption and routing systems than those previously used for processing checks. Legacy card issuers began offering similar services soon after. Because the card information had to be sent without the card being present, this raised many security issues.

The development of the 3D Secure 2.0 protocol soon followed. Similar to existing "Not-Present" transactions, identity became the primary means by which these functionally anonymous exchanges were assured. For card-not-present transactions, the original 3D Secure protocol provided an extra layer of security by requiring users to enter a password to confirm the authenticity of a transaction. This process soon proved to be cumbersome for users and led to low merchant adoptions as many were afraid that the friction introduced would lead to transaction abandonment. In addition, fraudsters were able to easily obtain the additional credentials from users via phishing and malware.

3D Secure 2.0 was introduced in 2016 to address many of the legacy issues of the original protocol around customer convenience as well as account for the proliferation of smart devices and new authentication methods. As card issuers and merchants seek to adopt 3D Secure 2.0, card-not-present fraud continues to be a challenge. According to Aite Group, card-not-present fraud will account for $4.4 billion in losses in 2018 in just the U.S. alone, increasing nearly 50% to $6.4 billion within the next three years.[2]

THE NEXT EVOLUTION: HUMAN-NOT-PRESENT

With all of this context established, responsible minds among the identity-assurance and anti-fraud set have begun to see a familiar theme emerging in business and technology. The modern techno-philosophy seems to be moving rapidly toward increased frequency and depth of automation directed toward tasks that traditionally required human participation. AI, machine learning, and the IoT are giving rise to a new age, one consisting of "Human-Not-Present" transactions.

If examined through the lens of history (and maybe pop culture as well), these innovations seem to have the potential to bestow untold boons on industry and civilization, while simultaneously possessing the potential to threaten the pillars of civilization itself. In a practical sense, this may today be a dystopian fantasy reserved for science fiction, but given the pace of innovation and the challenges already seen in cybersecurity and anti-fraud efforts, it is not inconceivable to predict that a humanless financial system will create a whole class of unforeseen problems, piled on top of those that are already imaginable and those we're witnessing today.

[1] https://www.britannica.com/topic/credit-card

[2] https://www.statista.com/statistics/419628/payment-card-fraud-losses-usa-by-type/

For example, the proliferation of "smart" devices has again preserved identity's place at the forefront of the convenience/security debate. Virtual home assistants such as Amazon Alexa, as well as more comprehensive smart home technologies, are designed to integrate with other devices in the home, such as mobile devices, home computers, and even some utility meters and home appliances. Future iterations of these technologies could offer functionality to automate some (minor, at least in the beginning) decisions and related tasks, and these transactions will increasingly require access to the users' online banking or other digital funds. By effectively removing the human from these transactions, transitive trust must carry the burden of identity and decision, and likely with little context and limited oversight by the not-present human, who will be the one to experience the pain when the system inevitably fails.

CONCLUSION: BE PRESENT

The world financial system, to say nothing of its public participants and supporting industry, has a major stake in the ways in which we conceive now of this new, automated age. Fortunately, we have the benefit of history and the lessons learned through the evolution of "payment-not-present" practices and the technologies that enable then. As such, it is critical that we seriously strive to learn from those lessons, and ensure that, while we embrace the convenience and freedom that automation can provide, we are also doing everything possible to ensure the probable risks are accurately assessed and mitigated. We should continue to understand, invest in and improve identity's role and effectiveness in all transactions, and also understand the gaps it leaves. To be ready for the "human-not-present" evolution, then, is to be present now, when such foresight and discipline will do the most good.

ABOUT THE RSA FRAUD & RISK INTELLIGENCE SUITE

The RSA Fraud & Risk Intelligence Suite helps organizations manage fraud and digital risk across multichannel environments without impacting customers or transactions. The suite offers risk-based authentication and behavior analytics solutions for web, mobile and e-commerce as well as fraud intelligence services to allow organizations to protect their customers across the entire digital journey. The Fraud & Risk Intelligence Suite is deployed at over 5,000 global organizations and protects over 1.5 billion consumers.