iovation®
A TransUnion® Company

2019 FINANCIAL SERVICES REPORT

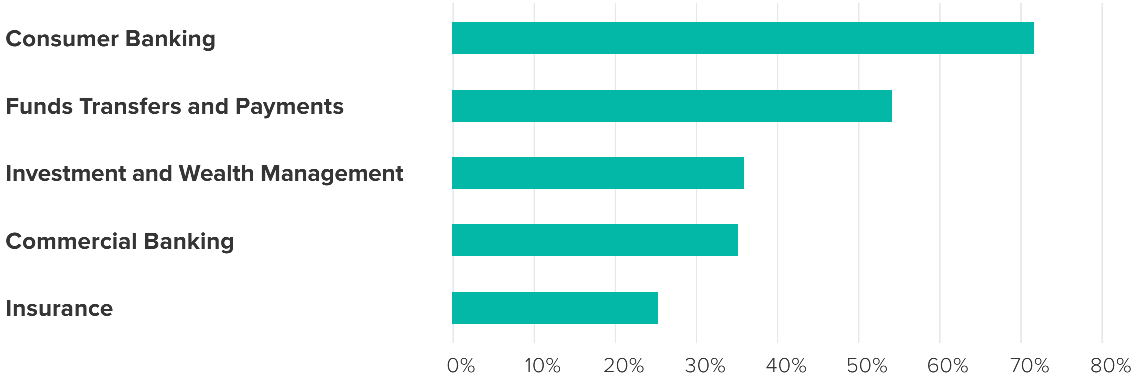
The Changing Face of Online Banking and Financial Fraud

Introduction

2018 continued a period of dramatic change for banks and financial institutions, and the pace and extent of change shows no signs of slowing down in the next few years. New technologies have put financial services at consumers' fingertips. Cybercrime in financial sectors is evolving. And traditional brick and mortar businesses are facing competitive pressures from upstart online technical financial service providers.

Financial Sectors Likely to be Disrupted by Fintech [2019-2024]

Data Source: PWC, Redrawing the Lines: FinTech's Growing Influence on Financial Services, 2018



The competitive war will be won by winning over the consumers, customers who are becoming more knowledgeable regarding fraud protection and who are demanding a smooth online experience. That means that banks and financial institutions need to demonstrate that they are protecting the business and customers from fraud without affecting the online experience.

Partners in Cybercrime Prevention

In the course of conducting business, banks and financial institutions need to protect themselves and their customers against new and evolving threats in cybercrime. iovation joined the battle against fraud and cybercrime in 2004. With our device-based and risk-aware fraud prevention and dynamic authentication solutions, we help online businesses protect their assets and their customers from theft and fraudulent activity. We currently process five billion transactions per year for our financial sector businesses.

Financial Services:

May 2017 - May 2018

Financial Services Transactions as Percent of All Traffic

56 Percent

Volume of Transactions

4.8 Billion

Number of Risky Transactions Stopped

31 Million

Reputation Reports Submitted by Analysts

1.4 Million

Fraud Attempts are Increasing and Are More Sophisticated: Are You Ready for the Future?

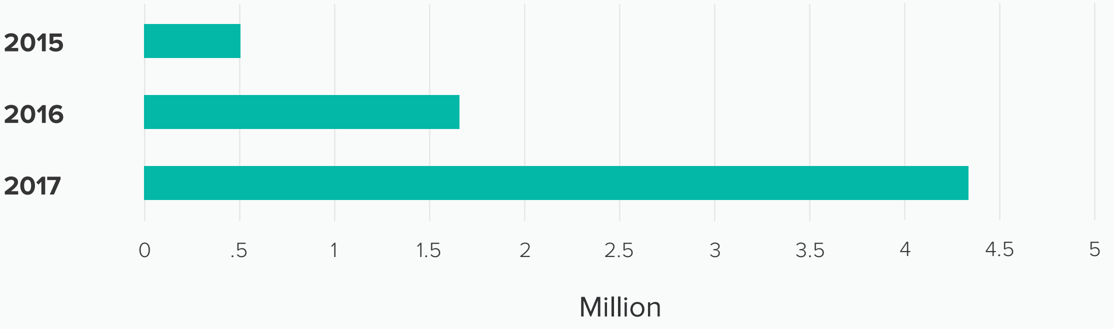
Cybercriminals are becoming more sophisticated and are evolving their techniques to take advantage of the increased digital and mobile presence of banking and financial services. Bot attacks, social engineering, phishing scams, malware, and use of synthetic identities are just a few of the unfolding techniques.

> Attempted fraud against bank deposit accounts reached $19.1 billion in 2016, up from $12.9 billion in 2014 – a 48% increase. Banks stopped about $16.9 billion in fraud attempts in 2016.” [1]
>
> As reported in Financial Regulation News, according to an American Bankers Association (ABA) report.

Increase in Online Banking Fraud Attempts

In iovation’s retail banking sector, while the total number of transactions rose by almost 20% in the last three years, the number of risky transactions caught rose by over 700%, indicating that fraudsters have been paying increasing attention to online banking. One reason that online banking is such an enticing target is because of the sensitive information accessible and handled directly by consumers.

Risky Transactions Stopped



[1] Financial Regulation News, www.financialregnews.com: Banking industry suffered $2.2 billion in fraud losses in 2016, Dave Kovaleski, Jan 2018

This rise in fraud attempts is being fueled, at least in part, by the flood of stolen identities and credentials available on the dark web. Since 2013, nearly 10 billion data records have been exposed.[1] The stolen credentials and availability of personal data are also driving a dramatic increase in account takeover (ATO) fraud.

Recent Data Breaches

26 Million

Exposed from the U.K. National Health Service (NHS)

198 Million

From Deep Root Analytics (a media firm contracted by U.S.)

200 Million

From the Motor Vehicles Department in Kerala, India

1.3 Billion

Through a breach of River City Media

57 Million

Records (both customer and driver) from Uber

50 Million

Records from Facebook

Changes in Identity Fraud: Synthetic Identities

Identity fraud has traditionally been categorized as first-party fraud, where a person commits fraud using their own identity, and third-party fraud, where a person commits fraud using someone else's identity. First-party fraud can occur when a customer applies for credit using their their real identity with no intention of ever paying it back. In comparison, third-party fraud, predominantly ATO fraud, happens when fraudsters impersonate existing accounts using credentials obtained from the dark web, through Remote Access Trojans (RATs) or other sources.

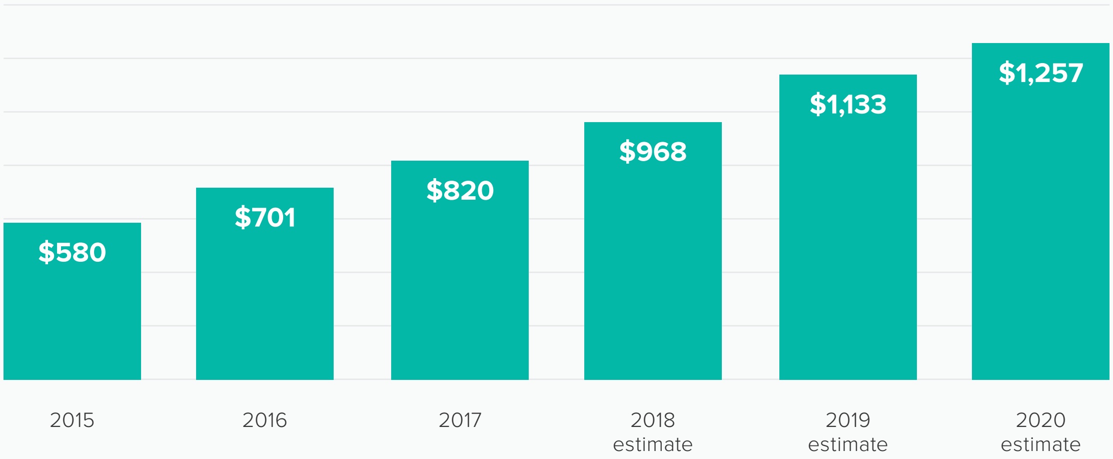
[1] Gartner: Market Guide for Online Fraud Detection, Jan 2018

Now we are seeing a marked increase in synthetic identity fraud, where fraudsters cobble together elements of stolen real identities with fake information to create a completely fictitious identity. A Gartner report found that there has been a dramatic increase in credit write-offs that can't be explained by a change in economic conditions. "Most of these new losses appear to be due to more sophisticated synthetic identity fraud and first-party fraud, which traditional identity proofing solutions and some of the older bust-out models fail to detect." [1]

Traditional fraud filters are not sophisticated enough yet at detecting synthetic identity fraud. When the synthetic identity thief applies for an account, they very often look like a real customer who has a limited credit history. According to a recent Aite report, credit card losses from accounts opened with fabricated identities reached $820 million in 2017, up almost 17% from the year before. And Aite forecasts the losses to rise another 53%, to almost $1.3 billion, by 2020. [2]

The Growing Losses from Credit Cards Opened by Nobody Real

Millions of Dollars Lost on U.S. Credit Card Accounts Opened with Synthetic Identities



Data Source: Aite Group, May 2018

[1] Gartner, The Growing Problem of Synthetic Identity and First-Party Fraud Masquerades as Credit Losses, March 2018

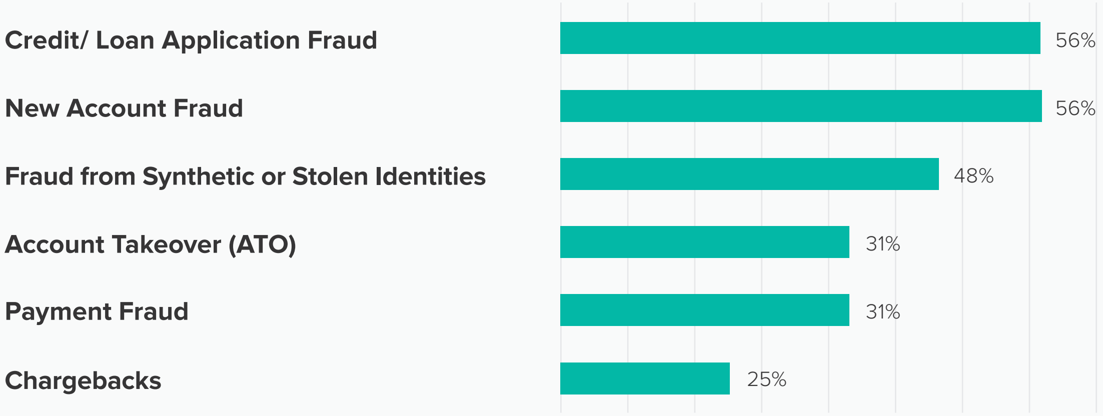
[2] Credit Card Losses From Synthetic Identity Fraud Jump, CreditCards.com, Sabrina Karl, May 2018

With synthetic identity fraud, often there is no real end user to notify the financial institution of fraudulent activity on their account. Or the owners of the real identities from which elements were stolen to create the fictitious identity did not suffer any direct financial loss, therefore these thefts are often miscategorized as chargebacks. That is one reason why synthetic identity theft is the fastest growing type of ID fraud, surpassing true identity fraud. Another reason is that there usually isn't any fraud history associated with the new identity, making it very difficult to detect. An ID Analytics study stated that synthetic identity fraud currently accounts for 80-85% of all identity fraud. [1]

Is Personal Identity Enough for Fraud Prevention

Two of the most prevalent categories of online fraud – account takeover and synthetic identity – use personal credentials to initiate their fraudulent activity. With a glut of personal information already available for fraudsters on the dark web, basing fraud prevention on personal identification alone is no longer sufficient. Similarly, digital identities, based on login credentials such as username and password, are not sufficient by themselves to authenticate high-risk transactions. The most comprehensive fraud prevention solutions, especially where high assurance is required, can include a combination of personal and digital identity verification along with multifactor authentication.

TechValidate - Challenges Experienced Before iovation



Data Source: Tech Validate survey of 52 users of iovation. Sample comprised of Financial Services customers.

[1] www.cnbc.com, Scammers create a new form of theft: 'Synthetic-identity fraud', Annie Nova, June 2018

The Fraud Picture in Financial Services

When a synthetic identity is used to commit fraud, it can appear on the surface as first-party or true identity theft. Analyzing fraud statistics can be problematic. For example, an iovation survey demonstrated that the two most prevalent fraud types that iovation financial services customers were dealing with before implementing iovation were credit and loan application fraud and new account fraud (56%), followed closely by synthetic/stolen identity fraud (48%). Increasing in rank was ATO fraud (31%).

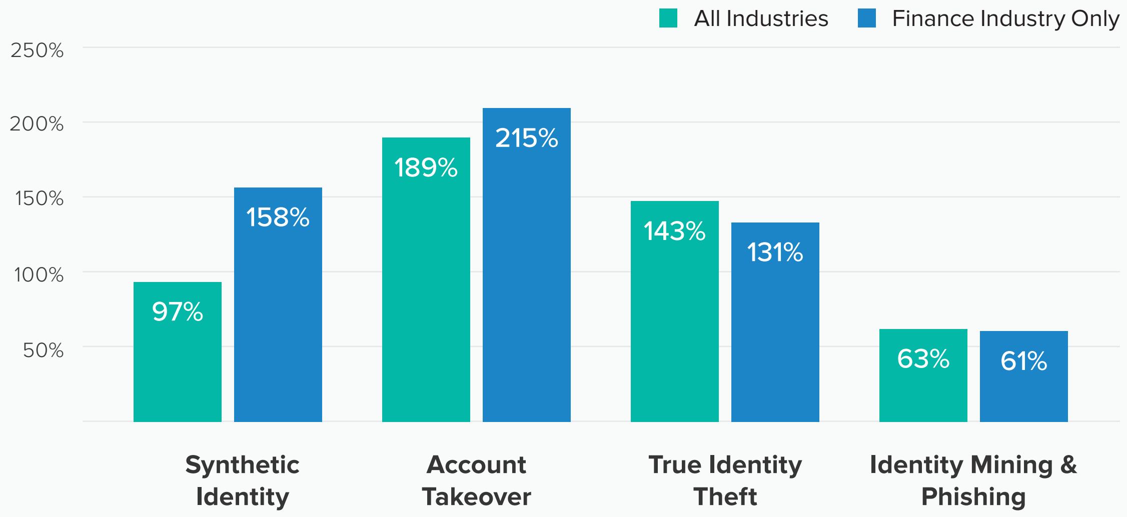
A fraudulent credit or loan application attempt or new account fraud could very well have been a synthetic identity attempt. It is important to examine fraud activity as a whole when determining your comprehensive fraud prevention strategy.

Businesses Plays an Active Role in Stopping Risky Transactions

iovation's extensive network of global clients and fraud analysts plays an active and integral part in detecting and preventing fraud. Between May 2016 and May 2017, financial services fraud analysts placed over 1.3 million fraud reports on accounts and devices in our network. Not only does a fraud report on a device or account indicate a potentially risky transaction, clients can consider the type of report when deciding on how to handle the transaction request – allow it, review the request or deny it outright.

Increase in Fraud and Abuse (Reputation) Reports

January 2015 - December 2017



iovation customers' reports of identity-type fraud incidents have increased significantly, especially in the financial sector. In the period from January 2015 to December 2017, reports of true identity theft rose 131%, reports of synthetic identities rose 158% and reports of account takeover fraud rose 215%.

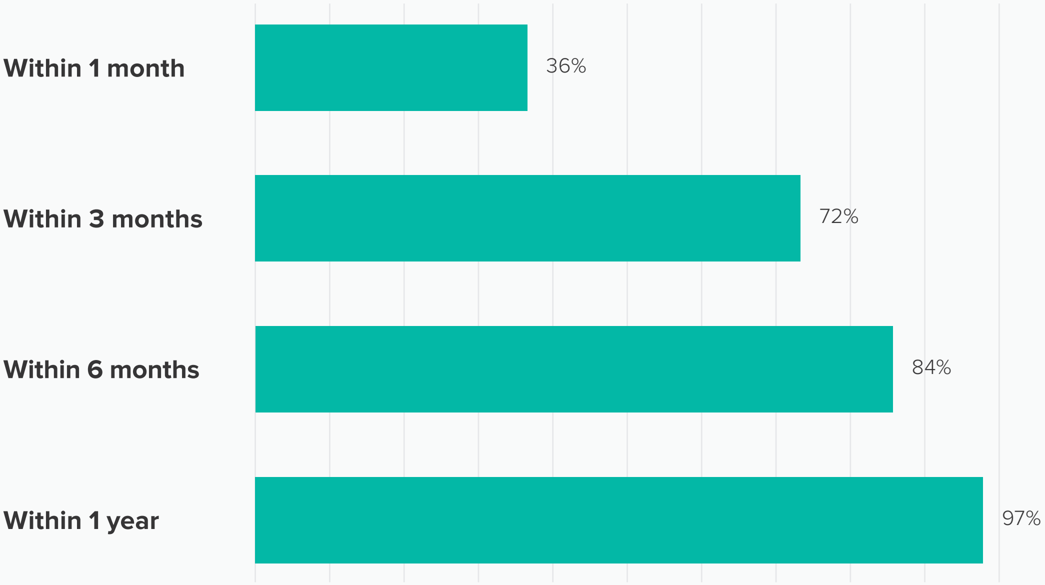
Fraud Protection - Good for the Bottom Line

ATO and synthetic fraud attempts look like they are coming from legitimate customers. So, the strongest protection will come from authentication solutions that verify the pairing of the customer's device to the account and employ mobile multifactor authentication, and device-based risk-aware fraud solutions that can check for any anomalies or red flags on the originating device.

We asked our financial sector customers how long it took before they realized a return on their investment in iovation fraud and authentication solutions. Over one-third of new customers saw ROI within one month. Over 70% realized an ROI within three months and that number jumps to 97% within the first year. A comprehensive fraud protection solution does indeed pay for itself, and quickly.

97% of Financial Services Customers See ROI Within One Year

How quickly did you see ROI after implementing iovation?



Data Source: Tech Validate survey of 33 users of iovation. Sample comprised of Banking and Financial Services customers.

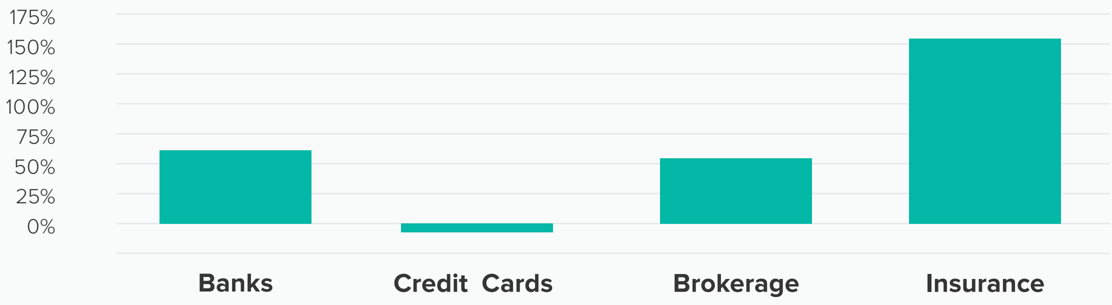
Don’t Forget the Call Center

Deploying a sophisticated online fraud detection and prevention solution is absolutely essential for banks and financial institutions to protect their business and their customers from fraudulent activity. But they can’t stop there. As fraud prevention solutions become more sophisticated and better at deterring fraudsters, cybercriminals are moving to other, less secure channels. As such the contact or call center has become a prime target. Fraudsters are using social engineering, more sophisticated spoofing techniques and SIM swapping schemes to evade traditional security processes. According to a Pindrop report, fraudulent calls to contact centers increased across the financial services sector from 2015 to 2016. [1] The one exception is in credit card issuers where the fraud rate remained high but relatively constant.

Financial institutions need a two-pronged policy focusing on both online transactions and call center activity to prevent fraud attacks in the future.

Increase in Call Center Fraudulent Calls 2015-2016

Millions of Dollars Lost on U.S. Credit Card Accounts Opened with Synthetic Identities



Keep Your Customers Happy with a Great Online Experience

With identity fraud increasing and evolving, financial institutions must have an effective way of detecting and preventing fraudulent activity. Customers want assurance that their transactions and personal data are safe from fraudsters. At at the same they are demanding faster, more convenient access to all products and services that the business has to offer. A DBR Research study found that enhancing the digital experience for customers is a critical priority with 72% of survey respondents putting it at the top of the list. [2] So the question is, how do you authenticate your customers and prevent fraud while still providing a hassle-free online experience?

[1] Pindrop, 2017 Call Center Fraud Report
[2] DBR Research, December 2017 Retail Banking Report

> Millennial customers recently reported switching their primary bank at a rate that is 2.5 times more often than Baby Boomers and Traditionalists and 1.5 times more than Gen Xers.[1]

The answer is to use the customer's device itself as an authentication factor. When a good customer returns to a site with a known device, you can use the device as a security factor and log the customer in without requiring any additional steps such as Captcha or KBA questions. Even more powerfully, because customers always have their mobile devices with them, you can use security factors directly on those devices without adding undue friction; authenticating a transaction at a website or even an ATM may be as simple as completing a facial recognition scan on a mobile phone.

Protect Your Business and Your Customers to Lead the Competition

The information in this report is a clear indication to banks and financial institutions about the need to implement comprehensive authentication and fraud detection that does not adversely impact the customer experience.

- To combat the evolving and increasing sophistication of identity fraud, such as the strong rise of synthetic identity fraud, deploy fraud and authentication solutions that verify devices and accounts and reduce friction through user-friendly tools such as mobile multifactor authentication.
- To help detect potentially risky transactions, deploy advanced fraud prevention solutions that provide a means for businesses to join together with other businesses to report incidents of fraud and abuse in one common location for everyone's mutual benefit.
- Deploying fraud and authentication solutions can quickly pay for themselves. Over 70% of iovation customers saw return on investment within three months of deployment.

[1] www.CSBS.org, Gallup Poll on Millennials and Their Banking Habits, April 6, 2018

ABOUT IOVATION

iovation, a TransUnion company, was founded with a simple guiding mission: to make the web a safer place for people to conduct business. Since 2004, the company has been delivering against that goal, helping brands protect and engage their customers, and keeping them secure in the complex digital world. Armed with the world's largest and most precise database of reputation insights and cryptographically secure multi-factor authentication methods, iovation safeguards tens of millions of digital transactions each day.

iovation
A TransUnion® Company

Global Headquarters

iovation Inc
555 SW Oak Street,
Suite #300
Portland, OR 97204 USA

PH +1 (503) 224 - 6010
FX +1 (503) 224 - 1581
EMAIL info@iovation.com

iovation.com