THE CHANGING LANDSCAPE OF IDENTITY FRAUD

giact®

The Changing Landscape of Identity Fraud

After years of steadily increasing fraud rates, in 2018 the cost of fraud and the number of victims impacted finally decreased for the first time in three years. The total amount of identity fraud in 2018 amounted to $14.7BB and impacted 14.4MM adults in the U.S. -- more than 5% of the total population.[1] However, identity fraud remains at historically high levels, despite the slight improvements of the past year. To further complicate the situation, there is an alarming trend of increasing losses for new account fraud (NAF) that showed a substantial 13% increase, costing consumers more out-of-pocket.

Figure 1: Identity Fraud Overall Metrics by Survey Year

Overall	2018	2017	2016	2015	2014	2013
U.S. adult victims of identity fraud (millions)	14.4	16.7	15.4	13.1	12.7	13.1
Fraud victims as % of U.S. population	5.66%	6.64%	6.15%	5.30%	5.20%	5.40%
Total one-year fraud amount (billions)	$14.7	$16.8	$16.7	$16.0	$16.7	$20.0
Total resolution hours (millions)	124	146	105	73	161	131
Mean fraud amount per fraud victim	$1,016	$1,032	$1,086	$1,220	$1,308	$1,526
Mean consumer cost	$117	$102	$50	$59	$123	$123
Mean resolution time (hours)	9	9	7	5	8	10

Source: Javelin Strategy & Research, 2019

Identity fraud has entered a new phase. While existing card fraud and account fraud have both decreased in frequency, fraudsters have shifted their focus to high value, less fortified areas that are more susceptible to NAF -- specifically loan originations. Fraudulent actors are deploying proven tactics against new, less conventional targets, and they are succeeding. Even more alarming, these attacks are costing victims greater time and expense.

This white paper details six key trends from the 2019 Identity Fraud Study published by Javelin Strategy & Research that shows the migratory patterns of fraud and provides tactics for firms across multiple industries to bolster their defenses against emerging fraud attacks.

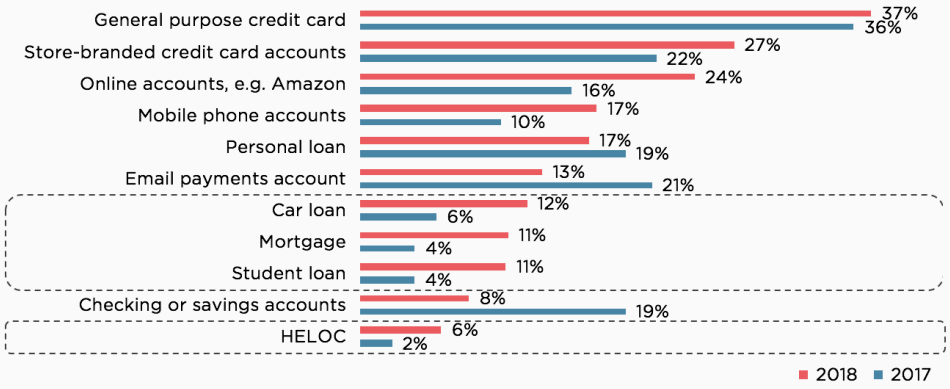
 © Copyright 2019 GIACT Systems, LLC

1.

TREND 1: Loan origination is the latest target

In 2018, existing account fraud, existing card fraud, existing non-card fraud, and account takeover all dropped below 2017 levels in terms of cost as well as the number of victims impacted. However, new account fraud increased by $400MM to $3.4BB, an increase of 13% while fraud overall dropped 13% [1]. As major financial institutions have invested in improving their authentication practices, fraudsters have shifted focus to areas that are less fortified and haven't previously suffered extensive losses. These areas include online accounts (e.g., eBay and Amazon), mobile phone accounts, car loans, mortgages, student loans, and HELOCs. Loan originations (car, mortgage, student, HELOC) showed particularly significant increases in fraud levels; rates more than doubled in each of these categories. [1]

Figure 2: Types of fraudulent new accounts opened (2017-2018)



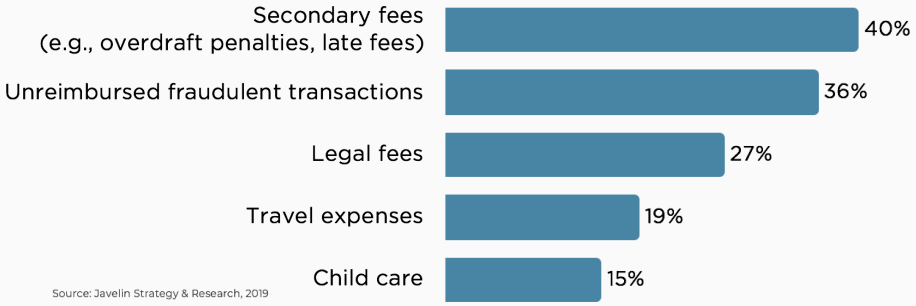
Source: Javelin Strategy & Research, 2019

2.

TREND 2: Victims of fraud are suffering more than in the past

While the number of victims has decreased in the last year, victims are suffering greater financial harm in the form of non-reimbursable transactions as well as out-of-pocket fees, such as overdraft charges, late fees and other costs. "In 2018, 23% of fraud victims had unreimbursed personal expenses for fraud, nearly three times the rate in 2016." [1] Additionally, the mean consumer cost of fraud overall increased from $102 in 2017 to $117 in 2018, an increase of 15%. [1]

Figure 3: Types of unreimbursed out-of-pocket expenses incurred by victims



Source: Javelin Strategy & Research, 2019

 © Copyright 2019 GIACT Systems, LLC

3.

TREND 3: Younger, less affluent victims bear a heavier burden in resolving fraud

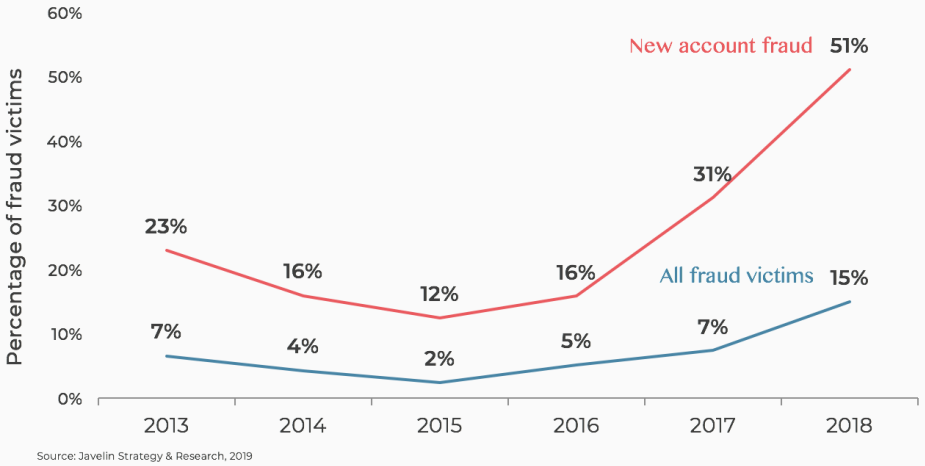
Not all types of victims suffer equally at the hands of fraudsters. While the total number of victims who incurred non-recoverable expenses more than doubled to 3.3 million individuals (or 20% of victims overall) from 2016 to 2018, they were disproportionately younger and lower income. Thirty-nine percent of victims who paid out-of-pocket as a result of fraud make less than $50,000 in annual income and more than half of them (52%) are under the age of 35. This trend is not surprising given the increasing frequency of new account fraud; younger, lower income groups are targeted for their identities, not for their existing accounts. [1]

4.

TREND 4: Familiar fraud is surging

Despite the robust U.S. economy, familiar fraud surged in 2018 from 7% to 15% of all fraud victims. When looking specifically at new account fraud, the increase was from 31% to 51%. [1] Because the perpetrators of familiar fraud typically have deep knowledge of the victim's identity and background, it is one of the most difficult types of fraud to identify using traditional authentication practices. It is also one of the costliest types of fraud for victims who are reluctant to pursue restitution from people they know. Three quarters of familiar fraud victims personally bear the cost of fraud losses. [1]

Figure 4: More Than Half of NAF Victims Personally Know the Perpetrator



Source: Javelin Strategy & Research, 2019

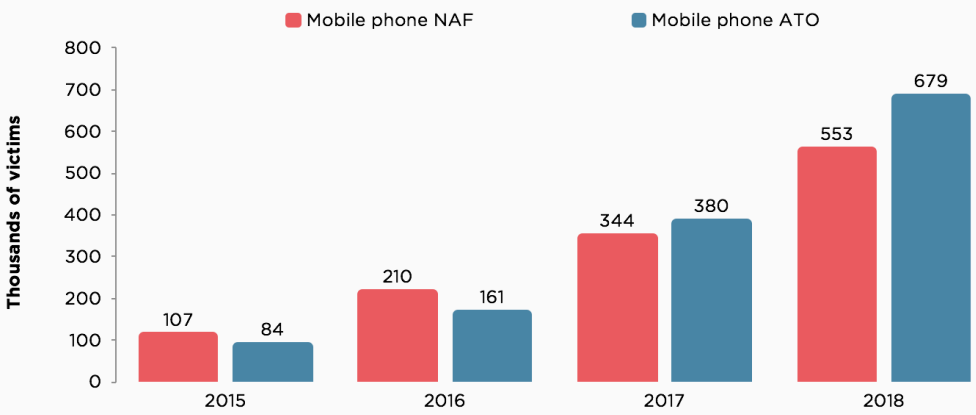
 © Copyright 2019 GIACT Systems, LLC

5.

TREND 5: SMS one-time passwords are a new source of risk

One of the most prevalent out-of-band authentication tools is a one-time use password delivered via SMS. Because of its popularity, this authentication method has become the latest focus for fraudsters who have developed sophisticated fraud tools to take over mobile phone accounts in order to intercept passwords as a very effective means of account takeover. The account takeover is accomplished using mobile malware that either intercepts and forwards text messages sent to the infected device or temporarily ports a number to a new device to steal the password so that the true account owner is unaware of the compromise. Mobile account takeover and NAF have skyrocketed the last four years. Mobile NAF has grown at a 51% CAGR since 2015 while mobile ATO has grown at a 69% CAGR.[1] Takeovers of mobile phone accounts and mobile wallet accounts are now greater than takeovers of email accounts and email payments accounts.[1]

Figure 5: Mobile phone account takeovers and new account fraud



Source: Javelin Strategy & Research, 2019

6.

TREND 6: Fraudsters are more successfully executing new account fraud

The longer fraudsters have access to accounts, the higher the risk for losses and the more damage they can do. In 2018, fraudsters increased the average number of days they had access to new accounts from 35.8 to 54.2, an increase of more than 50%. The jump in duration for NAF was the largest increase, but there were also increases in duration for account takeovers as well as existing non-card accounts.[1] Existing card fraud was the only category with a lower duration from the prior year, proof that the shift to EMV has pushed fraud into other categories.

 © Copyright 2019 GIACT Systems, LLC

Strategies to Counter Evolving Fraud Tactics

To counter the evolving tactics fraudsters are deploying, firms should explore the following recommendations.

First, lenders in particular should improve identity proofing as quickly as possible. As loan origination moves increasingly online, fraudulent loan originations will become more problematic. Even more alarming is that fraudulent loan originations can result in much higher losses than the typical credit card fraud, particularly with respect to mortgages, HELOC, and auto loans.

Second, stop relying on SMS one-time passwords and diversify authentication efforts to include more secure technologies. Specifically, in-app push notifications and out-of-band step-up biometrics are substantially more difficult for fraudsters to dupe. As mobile ATO continues to remain a focus for fraudsters, one-time passwords delivered via SMS will become increasingly at-risk. Firms should evolve their authentication approach to become less reliant on SMS. In situations where SMS authentication is necessary, verifying the consumer's phone number is essential to ensure that fraudsters haven't gained access to the mobile phone account.

Third, nonbanks are increasingly at risk to fraudulent attacks that target weak authentication practices. Rewards programs, merchants, mobile network operators and other online accounts are typically less protected than credit cards and bank accounts, and because of their lack of strong defenses, they are becoming more of a target as fraudsters look for weak areas to exploit.

1. Javelin Strategy & Research, "Javelin 2019 Identity Fraud Study," March 2019.

 © Copyright 2019 GIACT Systems, LLC

giact®

About GIACT's EPIC Platform®

GIACT is the only financial technology provider that offers a complete set of enrollment, payment, identity, compliance and mobile solutions built on a single platform – the EPIC Platform®. The EPIC Platform is a comprehensive solution that can be used via a single direct-connection API or a virtual web portal, giving companies a cost-effective way to defend against multiple types of fraud across the entire customer lifecycle.

The EPIC Platform's capabilities include:

- Single API integration allows companies to rapidly deploy customized solutions for enrollment, payment, identification, and compliance processes with minimal cost and operational disruption

- Positively identify consumer and business accounts using multiple traditional and non-traditional data sources to improve underwriting, risk management, and KYC process

- Real-time account verification and authentication of consumers and businesses, including funds verification, prior to customer enrollment or ACH payment processing to confirm status and verify funds availability before item processing

- Minimize unauthorized ACH and check returns, which are costly and damaging to a company's reputation

- Mobile authentication, identification, and verification in real-time across all customer touchpoints

- Ensuring OFAC and FinCEN Beneficial Ownership compliance with real-time processing while reducing false positives.

- Real-time identity verification and authentication of scanned ID's and check payments

For additional information on the EPIC Platform and functionality visit WWW.GIACT.COM.

 © Copyright 2019 GIACT Systems, LLC