

# JAVELIN

## 2021 Identity Fraud Study: Shifting Angles

23 March 2021 By: John Buzzard, Tracy Kitten

Javelin's 2021 Identity Fraud Study provides a comprehensive analysis of fraud trends in the context of a changing technological and payments landscape to inform consumers, financial institutions, and businesses about the most effective means for controlling identity fraud. The study began in 2003, and serves as the nation's longest-running analysis of identity fraud, with over 90,000 consumers surveyed.

This study is independently produced by Javelin Strategy & Research and made possible with support from the following sponsors:

### PLATINUM SPONSORS



### PARTNER SPONSOR

neustar

### INDUSTRY SPONSORS

feedzai IDInsight

## PERMISSIONS AND COPYRIGHT GUIDELINES

Only Platinum sponsors of this study are granted rights to use figures and data from the 2021 Identity Fraud Study in their marketing campaigns and external communications.

This report is copyrighted and may not be distributed. Javelin's Advisory Services clients do not have rights to cite any findings in their marketing campaigns, press releases, webinars, or any other external communications.

Javelin retains the ownership of the report, survey, raw data, methodology and all other project deliverables. While Javelin may grant other non-competing organizations rights to use the project's findings in other public venues, we retain ultimate discretion over such decisions.

## OVERVIEW

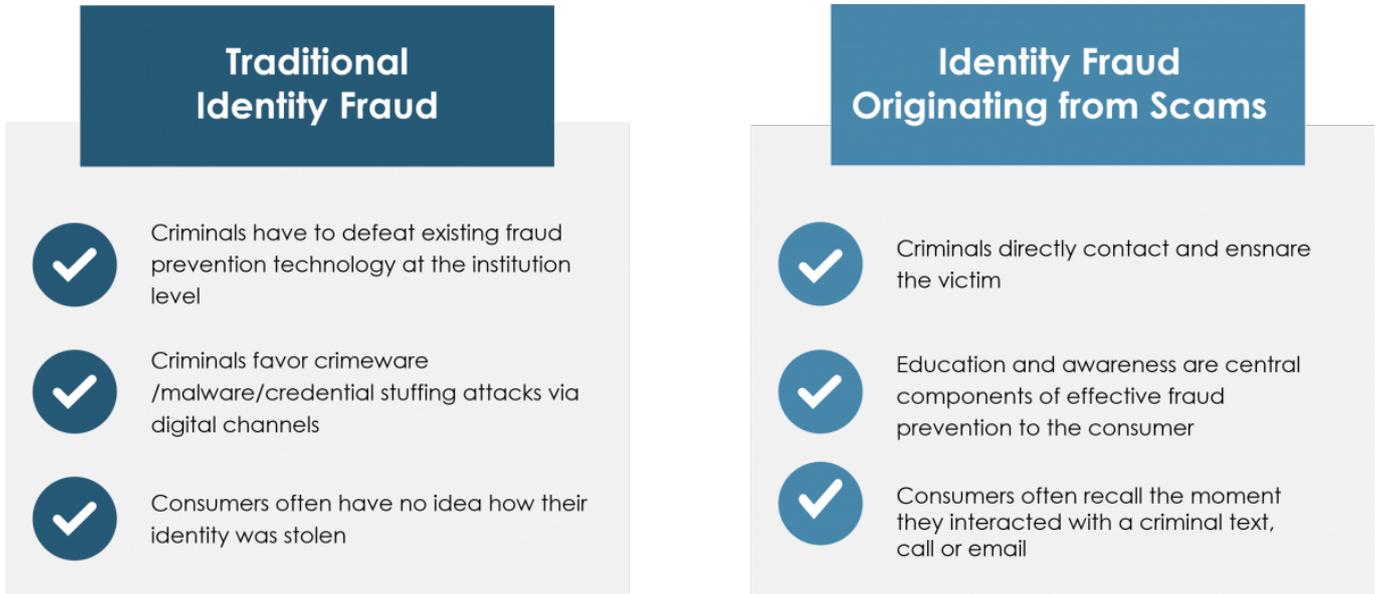
Since 2003, Javelin has researched the annual nuances of identity fraud. Identity fraud has quickly transformed through unique societal changes related to innovation, the COVID-19 pandemic, and criminal tactics that focus on corporate and consumer targets. As total identity fraud losses climbed to \$56 billion (USD) in 2020, it is important to make some distinctions between the two emerging types of attack vectors that criminals used in 2020 to perpetrate identity fraud.

Javelin has relied solely on the term identity fraud, without the need for further distinctions. As criminals focus intently on consumers as the path of least resistance in their quest to steal personal information, their tactics have changed. The routine theft and usage of consumers' personally identifiable information (PII) for criminal profit is still regarded by Javelin as traditional identity fraud. When it comes to traditional identity fraud, consumers have a scant perspective on the exact time and technique used by criminals to steal their information. They simply understand that a loss of PII

occurred, resulting in financial damage that they must resolve.

### Identity Fraud Tactics Diverge

Figure 1. How Identity Fraud Has Shifted



Source: Javelin Strategy & Research, 2021

A new and significant identity fraud threat was identity fraud scams that resulted in \$43 billion (USD) in losses to US consumers. Identity fraud scams are relatively easy to orchestrate and present an opportunity for criminals to bypass the fraud-detection barriers maintained by financial services providers, because they directly target the consumer. The consumer, within the context of identity fraud scams, becomes the path of least resistance. Access to the treasure chest of PII that enables criminals to take over consumers’ identities now becomes more tangible, because consumers continue to be vulnerable targets. A noteworthy characteristic of identity fraud scams is that consumers often recall the moment they interacted with a criminal through a text, call, or email.

In 2020, Javelin conducted a nationally representative online survey of 5,000 U.S. consumers to assess the impact of fraud, uncover where fraudsters are making progress, explore consumers’ actions and behaviors and how it relates to fraud risk levels, and identify segments of consumers most affected by fraud.

---

Copyright ©2020 Escalent and/or its affiliates. All rights reserved. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the permission of Escalent.