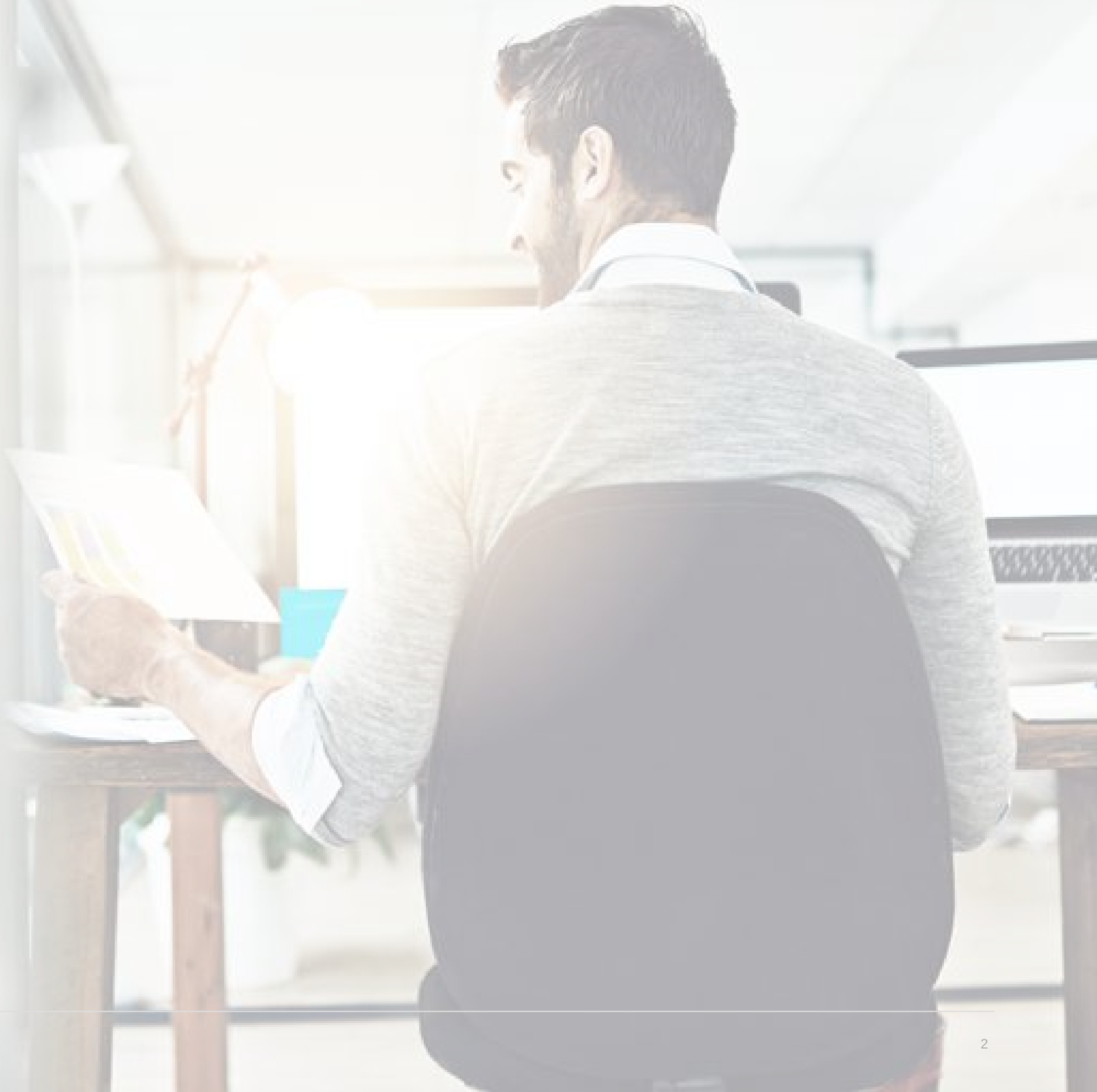
Drivers of identity risk fraud

The trends impacting account takeover fraud

experian™

Table of contents



What worked yesterday…

In the past, you could prevent fraud just by assessing identity risk at account opening.

Identity risk was confined to a single event, and exposure to financial loss was limited. A crook might spend the credit available on a fraudulently opened retail card or make bad deposits into a bank account and then spend the deposited amount before it was returned — but the damage was minimal.

What worked yesterday won’t work today…

Once confidence in the consumer’s identity was established, **risk moved away from identity fraud toward transaction-oriented fraud**. A card or checkbook might be stolen, but the consumer’s identity wasn’t considered a factor subject to compromise.

All of this has changed.

What worked yesterday won’t work today, and definitely won’t work tomorrow

With digital commerce, the individual’s identity and online credentials are the primary means of accessing deposits, borrowing money and making purchases. **Consumer identity is now a vulnerability.** Criminals don’t need to steal a debit card if they can log on to an account and transfer funds.

Access to consumer accounts is now identity-centric

We've moved from **single transaction fraud to identity-centric fraud** — and the damage is far from minimal.

In fact, **existing noncard fraud affected more than twice as many consumers in 2017 as in 2016** – Increasing at a record-high incidence rate of 2.52%.[1]

$5.8 billion

2017 existing noncard fraud

[1]*Javelin Strategy & Research,* 2018 Identity Fraud: Fraud Enters a New Era of Complexity, *Feb. 6, 2018.*

Secrets are no longer secret

Historically, there was some level of secrecy around our personal information. **Not just the details that make up our identities —** addresses, Social Security numbers, email addresses, phone numbers, etc. **— but where we bank, where we borrow, where we shop, what we like, and with whom we're connected.**

Breaches

Mass data compromises **have exposed much of our personal information** many times over. For many, their complete identities are known — with online activities monitored and mined.

The places where our identities are relevant — as customers, depositors, borrowers, investors, friends and family — may be accessible.

61.1 million

notified breach and fraud victims in 2017*

**Javelin Strategy & Research,* 2018 Identity Fraud: Fraud Enters a New Era of Complexity, *Feb. 6, 2018.*

Data, data, data

Criminals don’t need to steal every detail of information for some data theft to be useful. A vast network of hackers and thieves collaborate to buy, sell and share personally identifiable information which becomes powerful when combined.

4.2 billion

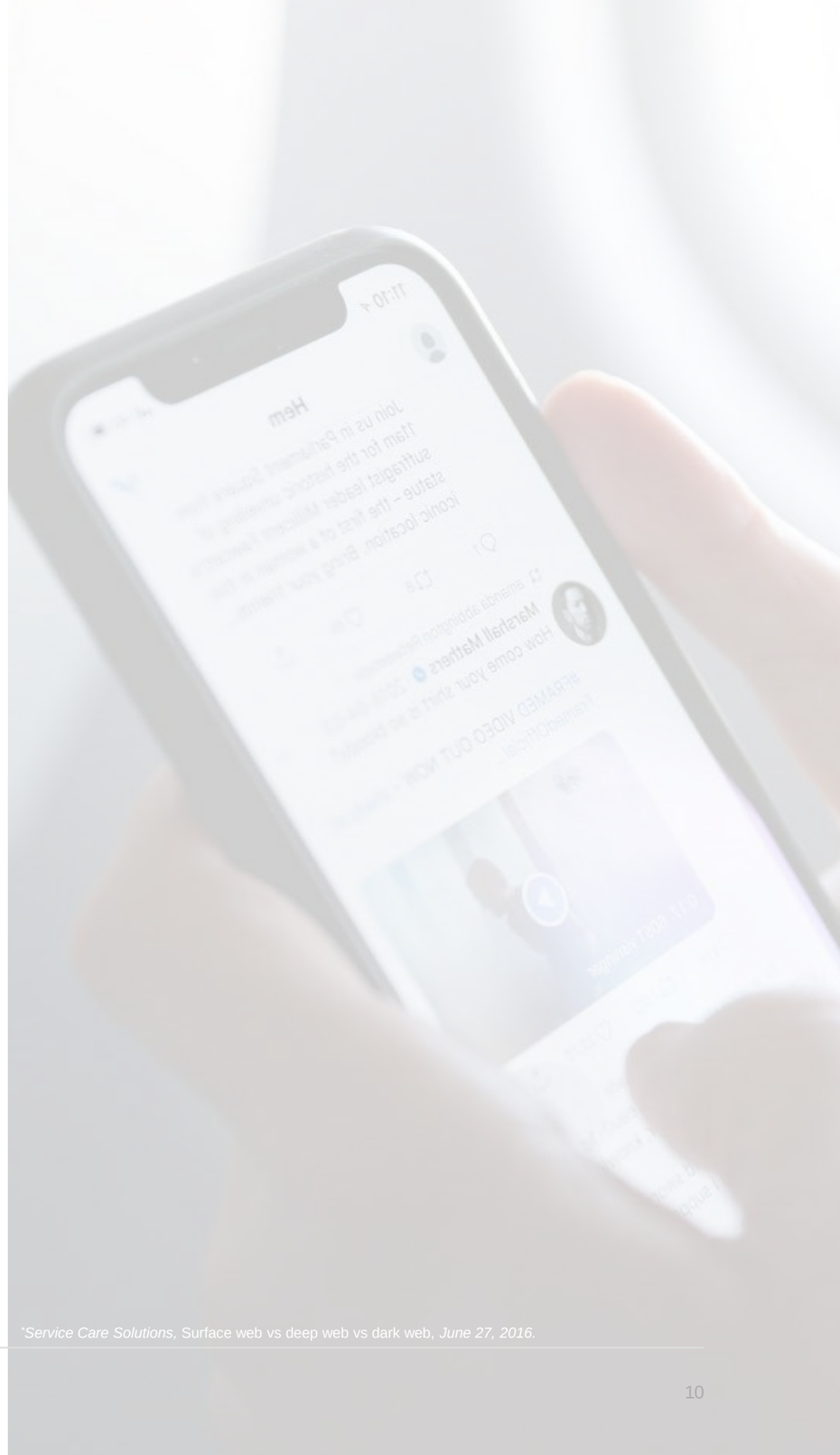
records disclosed in 2016

More than 4x the previous record*

**Javelin Strategy & Research*, 2018 Identity Fraud: Fraud Enters a New Era of Complexity, *Feb. 6, 2018.*

http:// The deep dark web

Below the surface of the visible web (the internet as we know it), there lies an unindexed dark web which hosts 95 percent of the content and an enormous amount of data that keeps illicit activities thriving.*



*Service Care Solutions, Surface web vs deep web vs dark web, *June 27, 2016.*

Two evolving ATO fraud schemes

1

Cross-account takeover

When fraudsters take over someone's account with a financial institution and elsewhere, like a mobile phone or email account, they're able to steal funds from those compromised accounts even in the face of sophisticated anti-fraud solutions.

It's a huge problem. In 2017, fraudsters increased their cross-account takeover efforts. This led to nearly three times as many consumers being affected by ATO in 2017 than in 2016 and losses grew to $5.1 billion – a 120 percent increase from the previous year. [4]

Two evolving ATO fraud schemes

2

Intermediary new-account fraud

Fraudsters are always adapting. The most significant shift in tactics during 2017 was the growth of intermediary new-account fraud. Criminals monetize a compromised existing account by opening one or more fraudulent accounts to take money from the victim.

In 2017, the prevalence of intermediary new-account fraud rose abruptly, reaching 1.5 million victims – more than 2½ times the previous peak of half a million victims in 2015.[4]

[6] *Aite,* Financial Institution Fraud Trends: ATO and Application Fraud Rising Rapidly, *May 31, 2017.*

Identities are only as secure as the weakest link

Our digital lives are interconnected. We link the pieces together whether the services are under one roof or not. Deposit banks are connected to credit cards, auto loans, investments, preferred retailers and others.

An exploited identity can do widespread financial damage. **A single weak link**, such as a call center, can let criminals use information they've gathered to impersonate a victim and gain access to and change credentials that connect to several sources of money.

The ‘word’ on passwords

Many people reuse their username and password combinations across multiple online relationships. Imagine that just one of those online relationships, such as a local homeowner’s association website, lacks the most current rigorous security measures.

When that site is hacked, usernames and passwords are exposed — **not just for this single account, but for many accounts.** Maybe even the account they have with your organization.

81%

of people surveyed use the same password across multiple accounts.*

36%

use the same password for 25% or more of their online accounts.*

**SecureAuth Corp.*, Survey: Majority of Americans Reuse Passwords and Millennials Are the Biggest Culprits, *July 9, 2017.*

The risk is constant

As our digital lives expand and become more interconnected, **we entrust our identities**, personal details and credentials to a growing list of online entities.

Every **new connection** introduces new systems and **access points that are vulnerable**.

38%

of financial institutions report an increase in account takeover attempts via the mobile channel over the past two years.*

**Aite,* Financial Institution Fraud Trends: ATO and Application Fraud Rising Rapidly, *May 31, 2017.*

Security is never a ‘one-and-done’

Controlling identity risk is no longer a one-time event. One right decision doesn’t ensure that your organization and customers are protected.

Identity risk accumulates through small, seemingly benign activities — a call center interaction that adds a new account holder, a change of a phone number or other contact information, a phishing email that collects one more piece of the puzzle.

While you are looking for one big, verifiable fraud event, criminals take over accounts through a slow drip of details.

47%

of financial institutions reported an increase in account takeover attempts.*

**Aite,* Financial Institution Fraud Trends: ATO and Application Fraud Rising Rapidly, *May 31, 2017.*

The secure experience

The most effective fraud prevention and identity strategy is the one that keeps people safe without disrupting the customer experience.

Your customers expect you to safeguard their information in ways that don’t waste their time, question their intentions, or force them to prove who they are each and every time they interact with you.

75% of consumers expect a consistent experience wherever they engage – on the web, social media or in person.[1]

87% of customers think brands should put more effort into providing a seamless experience.[2]

65% of respondents are frustrated with inconsistent experiences when they are using multiple channels.[3]

[1]Salesforce, 14 Retail Customer Experience Stats That Just Might Blow Your Mind, May 1, 2017.
[2]Zendesk, The omnichannel customer service gap, November 2013.
[3]Accenture, Global Consumer Pulse Survey, 2013.

The risk
today, tomorrow and…

Taking over existing accounts is a long game enabled by technology and known to criminals worldwide. You **can’t assume** that every presentation of an identity and credentials to access an account is being initiated by the identity’s owner.

But **authentication can’t be overly disruptive to the customer experience**. And it compounds the issue that so many of the risk drivers, such as mass data compromise, overexposed data on social media, reused passwords, poor data security and social engineering, lie outside our customers’ control.

This is what identity risk management in existing accounts has become. **The risk doesn’t end after an account is opened. It’s just beginning**. Just like the customer relationship.

The better you know your customer, the better you can stop fraud

A layered, proactive and passive fraud prevention and identification program can provide constant monitoring of customer interactions. It can also reduce false positive rates and allow you to truly get to know your customers' digital identities.

We recognize customers. We recognize fraud. We can help.

experian™

Let's talk