Theft in the Age of Digital Retail

Unlike shoplifting, no security alarm goes off when identity fraud is committed. In the age of digital retail, particularly in a post-breach world where millions of identities have been exposed, that should alarm most retailers.

Broadly defined, identity fraud occurs when a criminal (or "fraudster") steals someone's personal information and uses it to create an account or make purchases. Both in store and online, fraudsters are finding new and sophisticated ways to bypass retailers' fraud prevention measures and steal goods and services. At stake are a retailer's inventory, bottom line, and their reputation.

In this white paper, developed by GIACT®, the leader in helping companies positively identify and authenticate customers, we explore payment methods and vulnerabilities; the latest identity fraud schemes targeting retailers; and what retailers can do to improve their identity verification process and mitigate fraud.

Payment Technology

The digital marketplace and social media have made purchasing goods easier than ever before. Retailers accept a variety of payment methods: credit cards, debit cards, branded store cards and mobile wallets. But while all have resulted in great convenience for the consumer, they can also be compromised.

The identity threat creates a conundrum for a store associate who is being asked to open new credit card account: what if the shopper standing in front of them is applying for the account using stolen information? The very same networks that give the associate the ability to instantly open an account also allow thieves to defraud the retailer.

3.2 million adults fell victim to NAF in 2018. Meanwhile, NAF losses reached a staggering $3.4 billion in 2018.

As the use of secure EMV-embedded credit cards (i.e., chip cards) have spread, thwarting would-be criminals, fraudsters have begun to migrate from traditional banking products, instead opting to target store-branded cards and e-commerce sites by opening new accounts using fraudulent information — a tactic known as new account fraud (NAF). And according to new research, this tactic has proven successful.

The total losses from NAF are rising, according to Javelin Strategy & Research, which notes that some 3.2 million adults fell victim to NAF in 2018. Meanwhile, NAF losses reached a staggering $3.4 billion in 2018, up from $3 billion in 2017. Of that, general purpose credit cards comprised 37% of fraudulent new account openings, followed by store branded cards at 27%.[1]

E-commerce sites aren't immune, either: a 2019 study from Juniper Research reported that retailers are predicted to lose approximately $130 billion in digital card-not-present fraud between 2018 and 2023.

New Identity Fraud Schemes

Unfortunately for retailers, data breaches have made the job of identity validation more difficult. According to the Identity Theft Resource Center's (ITRC) annual report, "The number of U.S. data breaches tracked in 2019 (1,473) increased 17% from the total number of breaches reported in 2018 (1,257)." The ITRC report also notes that more than 1.65 billion records have been exposed in the past 15 years (from January 1, 2005 to December 31, 2019).[2] With all of this exposed data, it can make validating the true identity of your customer more difficult. Fraudsters know this — and are taking full advantage.

Fraudsters have become more sophisticated at wielding stolen identities, using one of two methods to create a new account: synthetic identity fraud or true name fraud.

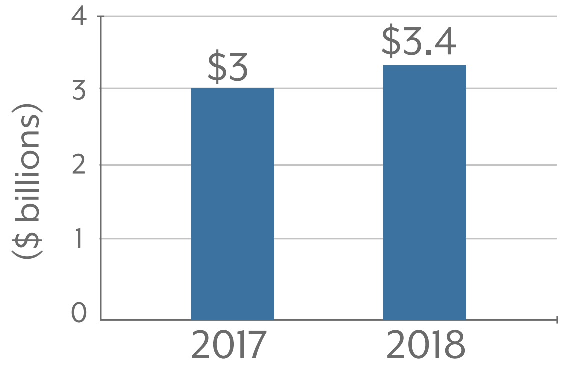
Synthetic identity fraud occurs when a fraudster couples legitimate and fictious information to create an identity. For example, a fraudster may create a fictitious identity by stealing a victim's actual name and SSN (often from vulnerable groups including children, the elderly and the homeless) and combining it with a fake address and date of birth. This type of fraud is particularly difficult to spot because some of the information is genuine, and there is no easily identifiable victim(s) (at least in the short term).

True name fraud is a more blatant identity theft tactic. In this scheme, a fraudster may use a real person's name and account to commit fraud. This type of fraud can be accomplished by stealing a victim's identifiable information and using it to open an account.

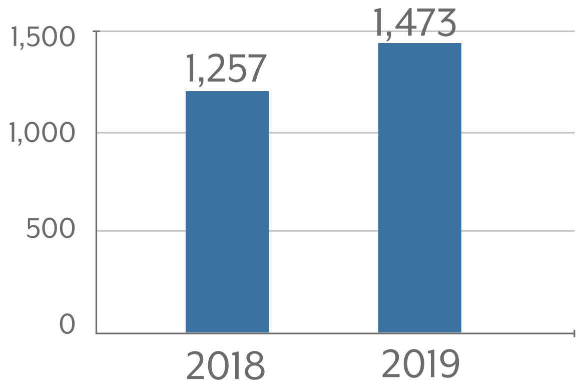
In both instances, fraudsters are accessing just enough data to deceive a retailer into handing over merchandise for which the retailer will likely never be paid.

Fortunately, there's a solution to validate the true identity of your customer.

NAF Losses Are Staggering



U.S. Data Breaches Up 17% YoY



How To Validate The True Identity of a Customer

To counter the above fraud tactics, retailers must adapt. First, they should improve their identity-proofing process as quickly as possible. As retail moves increasingly online, fraud will become more problematic. Second, retailers should not rely on card account information alone as the sole means of identity verification and should diversify authentication efforts. Overall, retailers must evolve their authentication approach and become less reliant on traditional methods.

One area for immediate improvement that can be made is the use of multi-factor authentication, i.e., using multiple data sources and approaches to validate identity. The appropriate multifactor authentication approach should be tailored to the retailer's needs.

For example, for store-branded cards, an effective application initiation process should fulfill two important requirements: 1) it ensures strong authentication of customer's identity, and 2) it provides a digital starting point for ongoing identity monitoring that allows the retailer to triangulate and compare identity factors as new information comes in.

For digital purchases (whether from an existing account or guest check out), in addition to validating the card holder's basic information, retailers should use a diverse set of data points, processed in the background, that includes both traditional and non-traditional data sources. By triangulating both traditional and non-traditional data, retailers will receive a more accurate picture of the true identity of the customer. This multi-pronged approach also makes it harder for fraudsters to dupe the system since it incorporates social media profiles, email addresses, mobile phone numbers and other data.

1. Javelin Strategy & Research, "Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt," March 2019

2. Identity Theft Resource Center, "2019 End-of-Year Data Breach Report," January 2020

About GIACT

To learn more about how you can more accurately verify the identity of your customers, visit **www.giact.com** or call **844-204-1417**.