TransUnion

INSIGHT GUIDE: FRAUD DETECTION

Now is the time for a fresh approach to detecting fraud

Learn where today's fraud detection falls short and what you can do about it. Read on.

Table of Contents

TransUnion

Now is the time for a fresh approach to detecting fraud

Times have changed, but fraud detection hasn't. Learn why most traditional fraud detection systems are falling short of financial services' needs and consumers' expectations.

While adequate for verification and screening, traditional fraud detection systems for new accounts are no match for today's sophisticated fraudsters. Worse, they force customers through confusing verification steps and unnecessarily delay access to their accounts, often for days.

A fresh approach can make your systems even more effective. Instead of asking more questions, gathering more personal details and forever adding more steps, let's rethink how we approach fraud detection so it prevents more fraud while it lowers customer frustration. This guide explains how.

Times have changed, so why hasn't fraud detection?

Traditional fraud detection methods must now contend with vast changes in the financial services landscape, many of which have been driven by the opportunities–and threats–from our hyper-connected economy:

- **Activity:** 61% of Internet users did their banking online in 2013, compared to fewer than 18% in 2000, according to the Pew Research Center.[1]
- **Customer expectations:** Today, people expect near-instant access to their new accounts, yet frequently must wait for days after they first apply online because current methods weren't designed for such speed.
- **Identity theft:** Last year, 13.1 million consumers experienced identity fraud–500,000 more than just a year earlier, according to a study conducted by Javelin Strategy & Research.[2]
- **Super-empowered fraudsters:** Using masked computers, stolen identities and clean addresses, a single person can apply for dozens of accounts across the country in just a few hours.

Traditional verification systems: Not made for these times

Traditional approaches to new-account fraud detection are verification systems. They were first created in the early 2000s, when opening accounts online was in its infancy and in the wake of new know-your-customer (KYC) rules. In addition to verifying consumer details, they check consortium data or other sources of suspect information–addresses associated with fraud, consumers with a history of fraud, Social Security numbers of deceased people, addresses that are mail drops or high risk and credit files with alerts–to identify red flags.

While this process for satisfying KYC regulations does prevent some fraud, it was not designed for today's business challenges and consumer preferences. Rather, it was developed to meet FACT Act requirements that institutions check personal information and factors, including alerts consumers place on their credit files before opening an account; and USA PATRIOT Act requirements that institutions document reasonable belief that the person with whom they are entering into a relationship is who she or he claims to be.

A new address: Red flag or false alarm?

To see these shortcomings in action, consider the path of two consumers applying for a line of credit, as seen with a traditional fraud detection system:

CONSUMER ONE	CONSUMER TWO
All application data matches verification databases except the address	All application data matches verification databases
No high-risk flags for past fraud	No high-risk flags for past fraud
Using a new address–one that's 500 miles from where he has lived for the past six years	

Which of the two presents a higher fraud risk? Traditional approaches would require manual intervention with Consumer One, but would let Consumer Two pass through. Now, consider additional unrevealed information about Consumer Two:

- → The identity has existed for only about a year, despite a stated birth year of 1974
- → The identity has been used to apply for multiple credit products and mobile phones in the past 30 days
- → The identity's address is not on a hot list, but is being used by six other identities, all actively seeking new accounts
- → He is applying with a computer that has opened nine other accounts in the past week
- → His computer has been configured to evade tracking and profiling

Given this more complete picture, what initially looked like a low fraud risk is almost certainly a fraudster. And yet, although the financial institution met its compliance obligations, it was nonetheless exposed to fraud.

Meanwhile, Consumer One endures a negative experience right from the start, despite the following facts in his favor that a traditional approach could not detect:

- → His identity has been used consistently and in a way that's low risk
- → He's using a known and trusted computer
- → He's applying using a mobile phone that's been tied to him for at least five years

But without knowing such favorable factors, Consumer One's line of credit cannot be opened right away; he may be required to speak with a customer service representative; and he'll probably need to email or fax additional documents to prove that he has indeed moved from the address on file to the address on his application.

Asking people to wait is asking them to leave

The plight of Consumer One clashes with the expectations of today's digital consumer: when online, people expect rapid responses and easy ways to access new accounts, whether for banking, social media, online shopping, and the like.

If required to jump through hoops or wait days for access to their new accounts, many applicants give up in frustration, never to return. Honest people pay the price in time lost and rising anxiety as we pile more and more steps onto the application process.

Given that the majority of cross-selling occurs within 90 days of a new customer opening his or her first account,[4] will a new customer who just endured an unfavorable experience be willing to engage in cross-sell conversations?

Super-empowered fraudsters: Exploiting weaknesses

Many institutions believe their fraud losses are under control, but today's fraudsters have more opportunities for criminal activity than ever before. In fact, many institutions are ill-equipped to detect threats from sophisticated organized crime rings. Criminals are increasingly aware of how to exploit weak links to maximize financial gain. Here are a few examples:

- **Mining for gold:** Millions of pieces of personal information are now stored collectively in databases, which are gold mines for hackers. In addition, social media encourages people to publicly expose personal details–even addresses, phone numbers and birthdays. In fact, the price of black-market "fullz"–consumer profiles with personal and financial data bought and sold by fraudsters–has plummeted by 40% in recent months, indicating a glut of supply.[5]
- **Exploiting human nature:** Fraudulent transactions are increasingly perpetrated using the call-center channel. The combination of relatively weak fraud detection, simple human error and the natural tendency to be helpful make call centers a prime target for manipulating accountholder information or establishing accounts that are later used fraudulently.
- **Criminals can afford to wait:** One tactic of criminals is to open a mobile phone account and other low-barrier accounts using a phony name and unused Social Security number. This allows them to slowly build up the identity's credit reputation, eventually putting them in a position to open–and defraud–multiple lucrative credit lines.

Our goal must be to dramatically improve the customer experience while also preventing more fraud

What will a fresh approach look like?

Given all the limitations of traditional methods, we must analyze how a customer is applying and look deeper into who he or she is. Using more predictive tools, financial institutions can spend less time on manual reviews, confidently make quick approvals and reduce fraud losses.

Our goal must be to dramatically improve the customer experience while also preventing more fraud by meeting these objectives:

- Prevent sophisticated fraud techniques, especially in faceless channels
- Check against real-time information
- Act behind the scenes, invisible to customers
- Require fewer steps for customers
- Give customers much faster access to new accounts

Next, we need methods that accomplish those goals and objectives. Here's a glimpse at how that can work, using the tools available today:

- **Identity behaviors:** We can now analyze identities, using real-time cross-industry data, to detect fraud that goes unnoticed by traditional verification tools. Gaining insight into how an identity is being used, how it relates to other identities, and examining other behavior patterns helps us pinpoint fraud risk and prioritize manual reviews.

- **Device verification:** Why not turn criminals' own devices against them? We can look at the computer or mobile phone used to open an account to examine hundreds of variables for anomalies and risk. Assessing risk factors and examining a device's reputation, then combining the data with what's known about a consumer, lets us make informed, contextual decisions. Importantly, it's done behind the scenes with little interruption to consumer transactions.
- **Identity authentication:** Quick yet effective, we can authenticate identities by using something applicants have (send their mobile phone one-time passcodes via SMS text) or by asking applicants something they know (using knowledge-based questions). This dramatically reduces customer friction by employing proven verification technologies for low-risk transactions.

Consider again Consumer One opening an account with an address that doesn't match his historical record. If an institution sees he's applying for only one or two accounts, is using a computer long associated with legitimate transactions, and easily enters a verification code sent to his mobile phone, the risk decision is much easier.

Although follow-up will still be necessary to complete compliance requirements, the process has moved from "we'll get back to you" to a decision to immediately approve the application. The results are fewer steps for the customer, faster approval (and fewer abandonments) and a far better experience overall.

Now is the time to start the conversations within your organization to take advantage of the new tools that could make your fraud detection system not just one that keeps fraudsters in check–but that also supports positive customer experiences.

NEW ADDRESS: BIG OPPORTUNITY OR BIG MISS?

When people move, they often apply for new checking and savings accounts, new cable TV accounts or new credit to finance home improvements. In 2013, 36 million Americans moved and up to 40% of some new account applications came from people with new addresses, according to TransUnion.[3]

This is a big opportunity for companies who offer a smooth, fast application experience–and a big miss for companies who don't. With a more holistic approach, when an address can't be verified, you have the ability to look to other factors–such as recent activity, cross-industry data, and the reputation and location of the applicant's computer–that help mitigate the unverified address.

Q: **We have the ability today to detect which of the following?**

a. That an identity of a person claiming to be 40 years old has existed for only 13 months

b. That an identity has been used to apply for multiple credit products in the past month

c. That an address tied to an identity is being used by six other identities, and all are actively acquiring credit

A: **All of the above.**

Works cited

1 Fox, Susannah. "51% of U.S. Adults Bank Online." *Pew Research Internet Project*. August 7, 2013. http://www.pewinternet.org/2013/08/07/51-of-u-s-adults-bank-online/ (accessed May 22, 2014).

2 Javelin Strategy & Research. "A New Identity Fraud Victim Every Two Seconds in 2013 According to Latest Javelin Strategy & Research Study." February 5, 2014. https://www.javelinstrategy.com/news/1467/92/ANew-Identity-Fraud-Victim-Every-Two-Seconds-in-2013-According-to-Latest-Javelin-Strategy-Research-Study/d,pressRoomDetail (accessed May 22, 2014).

3 TransUnion. From data in the TransUnion consumer credit database.

4 Tschida, Teresa. "The Importance of That First Embrace." *Gallup Business Journal*. November 10, 2005. http://businessjournal.gallup.com/content/19606/importance-first-embrace.aspx (accessed May 22, 2014).

5 Clarke, Elizabeth. "The Underground Hacking Economy Is Alive and Well." Dell *SecureWorks*. November 18, 2013. http://www.secureworks.com/resources/blog/the-underground-hacking-economy-is-alive-and-well/ (accessed May 22, 2014).

LEARN MORE

More information on this topic at solutions.transunion.com/fraudprevention.

TransUnion

TransUnion