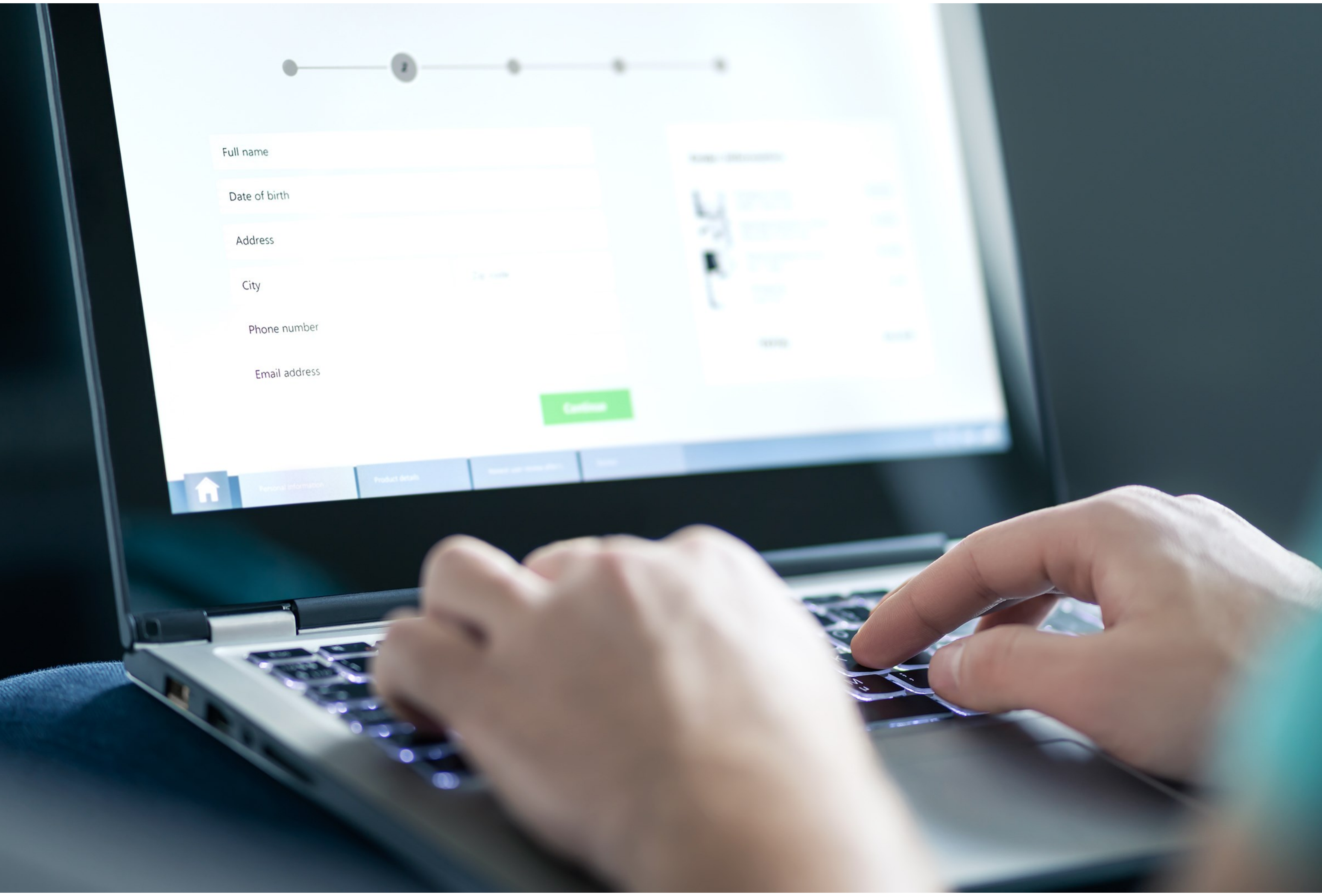
THEFRAUDPRACTICE
PROTECTING THE BOTTOMLINE



IS THIS *REALLY* A NEW USER? DETECTING FRAUD AND ABUSE AT ACCOUNT OPENING

White paper presented by The Fraud Practice

IS THIS *REALLY* A NEW USER? DETECTING FRAUD AND ABUSE AT ACCOUNT OPENING

Written by: Justin McDonald, Sr. Risk Management Consultant

A white paper by The Fraud Practice

Sponsored by Ekata, a Mastercard Company

Introduction

Many fraud and abuse events begin at the account opening or creation event, but assessing risk at this stage is a difficult balance. At the very beginning of the customer life-cycle journey, there is a need to be mindful of any potential friction. While it is natural to lean towards user experience at this stage, any fraud or abuse that can be snuffed out at an early point in the customer journey saves operational and screening costs that would occur later on the path to an eventual order decline or, worse, a fraud loss.

Ecommerce retailers, lenders, financial institutions, social media platforms, news and entertainment sites, email providers and any website or app offering a user account online must be concerned with the account opening or creation event. Many organizations, merchants in particular, tend to focus their risk screening efforts at the end of a customer's journey when they transact or engage in an event with the potential for direct financial loss. This means risk signals at account opening are often overlooked, or simply not collected, despite there being value in considering these signals at the nascent stages of a user's journey.

Direct, or "hard," fraud losses are the most noticeable and primarily occur at checkout or transaction events, but many of these begin with a synthetic identity provided at account creation. Promo abuse and other "soft" fraud schemes begin here as well, and are a larger issue than many organizations realize. According to a PYMNTS.com[1] study, nearly **three-quarters** of retailers report experiencing promo abuse, while total policy abuse is estimated to cost U.S. firms nearly **$90** billion per year.

The focus of this white paper is to discuss the different types of attacks and fraud that organizations face at the account opening event, as well as strategies to mitigate both hard and soft attacks pertaining to automated screening and manual processes.

Sources:
1 - https://www.pymnts.com/news/retail/2021/89-percent-retailers-get-burned-abuse-their-own-customer-promotions

Attacks and Abuse at Account Opening

Many fraud losses happen with established user accounts, not just guest checkouts. This could be legitimate user accounts that have been taken over, or from sleeper accounts created by fraudsters to build clout.

Fraud attacks and abuse at or adjacent to account opening events fall under two primary categories:

- **Hard fraud** attacks that result in direct financial loss and therefore are the most noticeable.
- **Soft fraud** is more akin to abuse, often flying under the radar. Perpetrators don't consider themselves to be fraudsters but rather just "gaming the system." Soft fraud schemes are typically more difficult to identify.

Soft Fraud and Abuse

Most types of soft fraud attacks that organizations are likely to encounter fall under the umbrella of **promo abuse**, which involves exploiting promotions offered by retailers. Specific types of promo fraud include:

- **Promo Code Abuse**
- **Free Trial Abuse**
- **Referral Abuse**
- **Loyalty Abuse**

Ekata's Identity Network Score helped a top APAC eCommerce marketplace detect over 80 percent of suspicious promo abuse attempts.

Promo code abuse is when users create multiple accounts with throwaway email addresses or other credentials to take advantage of discounts and promotions intended only for new customers or those newly signing up for a marketing list.

Promo abuse may or may not be associated with a new account opening. For example, a customer could always use guest checkout and each time sign up for the email marketing list with a new email address to receive a new, dynamic promotional code.

Soft fraud comes in many forms and is typically difficult to identify as it does not show up as a direct financial loss in most cases. As a result, many organizations are not able to measure the impact of soft fraud, which typically means do not take measures to combat it.

Free trial abuse takes advantage of customer acquisition strategies that offer a limited free trial upon signup. These programs typically require an active payment card to be provided, which will be charged for the first round of service after the free trial expires. Users abusing these offers cancel before the free trial rolls over into a paid subscription and then sign up with a new account, repeating the process until stopped.

Referral abuse involves one person or multiple people creating new accounts and transacting from those accounts to claim a financial incentive or loyalty points award to another account also under their control. “Refer a Friend” programs are a common customer acquisition strategy component, but their costs can be inflated while driving up perceived new user churn when these incentive programs are gamed by users.

Loyalty abuse refers to schemes where users exploit undesirable ways to rack up loyalty points, such as submitting orders before later canceling or returning them in hopes that the associated loyalty points won’t be clawed back. Ill-gotten loyalty rewards are eventually used towards the purchase of goods or services, which is ultimately a form of stealing. This should be differentiated from loyalty point theft, which involves account takeover to use or transfer legitimately earned loyalty rewards and is a form of hard fraud.

Hard Fraud

Organizations typically feel the pain from hard fraud attacks in the form of financial losses, but also, potentially, brand damage. Hard fraud schemes include:

- **Email Harvesting**
- **Monetizing Stolen Identities**
- **Monetizing Stolen Payment Credentials**
- **Utilizing Sleeper Accounts**

Email harvesting occurs at the account creation event, where fraudsters attempt to create accounts with email addresses they hope are already in the system. This often targets email addresses that have already been compromised in combination with an associated password. Once the fraudster confirms an email address is associated with a particular merchant, app or website, they send targeted, branded phishing campaigns and/or attempt account takeover with the password that was compromised along with the email address from a third-party data breach.

> ***Synthetic identities are used with guest checkouts or to create new accounts with a combination of compromised consumer payment and identity data as well as fraudster-controlled data points.***

Email harvesting has characteristics of both hard and soft fraud. It is like hard fraud in intent, where the perpetrator identifies as a fraudster and is taking actions to acquire information that will lead to explicitly illegal activity. Yet it is similar to soft fraud in how it so often flies under the radar, as the activity itself does not result in a direct loss but is a stepping stone to something larger.

Monetizing stolen identities is a form of synthetic identity fraud where a majority of the data points provided at account setup are taken from the stolen identity information of a victim consumer. This is among the most ifficult to stop as sensitive and complete information of the identity theft victim, including their Social Security or National ID number, are often compromised. This may involve taking a loan out in the victim's name with no intent of paying it back, or other methods to steal money using a consumer's identity. Since lending and financial services are often the target of such attacks, account opening is the de facto first step in the stolen identity monetization process.

Monetizing stolen payment credentials is a form of synthetic identity fraud where limited information belonging to the real payment account holder is available or presented. Compromised personally identifiable information (PII) may be limited to a billing address and the payment account or credit card number. Whereas a complete stolen identity is more likely to be used against lenders and financial institutions, when the compromised data is limited to a payment card account and ancillary PII, fraudsters are more likely to attempt purchasing goods or services with the stolen payment card data.

Synthetic identity fraud intended to monetize compromised payment credentials does not require account creation, as this can typically be conducted via guest checkouts. However, fraudsters often create user accounts with synthetic identities because they think doing so will lead to a greater likelihood of their order attempt being accepted versus a guest checkout. This can lead to fraudsters creating…

The amount of time a user account has existed should not be utilized as a positive risk signal if that account has not yet displayed legitimate activity.

Sleeper accounts, which refers to user accounts created with synthetic identities for the purpose of building rapport or trust. Often, these accounts are created weeks or months before being used to conduct transactions, as it is believed that the existence of a user account and the length of time the account has been in existence may be interpreted as a positive risk signal and increase the likelihood the fraudulent order is accepted.

Defending Against Soft Fraud and Abuse

It's a philosophical cliché. "If a tree falls in the woods and nobody is around to hear it, does it make a sound?" Similarly, if an occurrence of fraud or abuse does not manifest as a chargeback or direct financial loss, did it really occur? The answer to the second question is a definitive "yes." Just because certain tactics are hard to identify or don't show up as a loss, doesn't mean that they don't impact an organization's top and bottom lines.

Organizations can either turn a blind eye to these schemes and forms of abuse, or they can employ mitigation strategies which will pay dividends in the forms of lower customer acquisition costs, lower churn on new user accounts and other benefits.

Challenges

Customer acquisition costs are often inflated from return users abusing promotions and free trial offers. **Promo abuse** leads to inflated marketing costs, overstated incentive performance marketing metrics, understated new user retention, understated repeat buyer metrics, and ultimately a hit to revenue. Mitigation strategies can differ based on whether multiple user accounts are being created or the abuse focuses on providing new contact information to receive incentives for joining marketing lists.

Some email domains present challenges as they allow changes to the email root while sending to the same inbox. This is an issue with Gmail, for example, which is one of the largest free email providers. The same Gmail email address can include periods at any point within the email root, which can make the email addresses appear different but ultimately be delivered to the same inbox.

Would your organization see the following as the same email address or as many new and different users?

- FakeEmail@gmail.com
- Fake.Email@gmail.com
- F.akeEmail@gmail.com
- Fa.keEmail@gmail.com

These, along with many other possible variations, would have all email deliveries arrive in the same inbox.

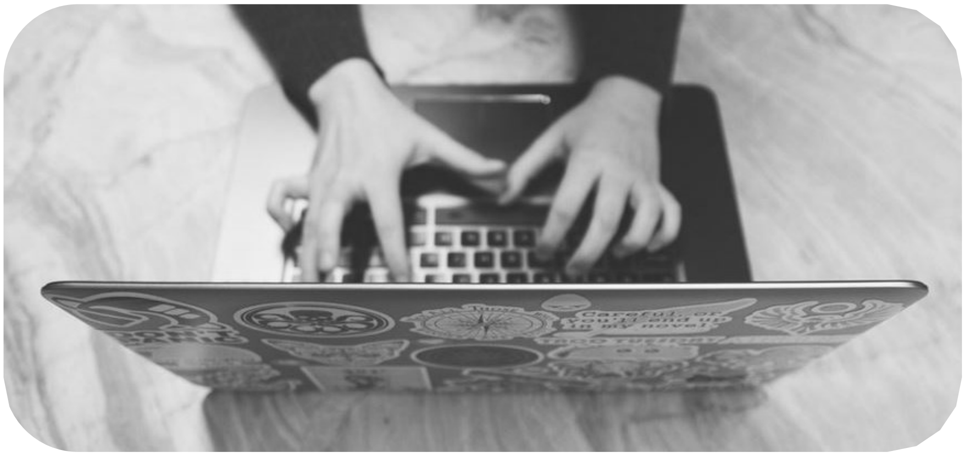
SMS text message marketing lists are easier to defend against this form of abuse as phone numbers are more costly to possess. Email addresses can be created quickly and freely, so it often makes sense to consider risk screening around the email domain and age of the email address.

Free trial abuse impacts top line revenue, as users who should become paying customers are able to enjoy services while evading payment. This typically requires creating a new account for each free trial period, therefore mitigation strategies should focus on linking and shutting down accounts associated with users who have already claimed the free trial.

Free trial offers that auto-enroll into a paid service are frequently targeted with card testing because fraudsters know that a successful authorization is required to begin.

Challenges can be seen around the reuse of a Gmail or other email address as discussed previously, or simply by creating completely new emails. Free trial abuse prevention can focus on other data points, such as the payment card used, but virtual credit cards or temporary card numbers, prepaid cards, or customers with many different payment cards at their disposal, can repeatedly appear to be new users.

Referral incentives abuse represents an explicit cost. Whereas free trial abuse is an implicit cost on revenue that could and should have been collected, referral incentive payouts represent a tangible expense, if not in the form of direct monetary compensation, then in some form of credit or reward. Similar to free trial abuse, there should be a focus on recognizing links between accounts, whether they are operated by the same person or multiple people working together.



Risk Mitigation Techniques and Strategies for Soft Fraud

There are many tools and strategies organizations can leverage to recognize and reduce these forms of soft fraud and abuse, and many of these techniques can be applied to multiple schemes. A helpful exercise is to look at the account creation event through the same lens as a transaction event, as many similar risk screening techniques can be utilized, such as identity screening and link analysis.

Ekata's Identity Engine synthesizes over 7 billion identity elements and 5 billion digital interactions globally that enable businesses to not only validate identity elements and how they are linked, but also analyze how these elements are being used online.

Link analysis should be performed at the user account level to recognize data points that have been reused or shared across multiple user accounts. This can include payment card numbers, billing and shipping addresses, phone numbers and passwords. Most organizations require unique emails per user account, but these repeat abuse users are likely recycling many other data points.

Link analysis can be performed manually, but it comes at an operational cost. Risk modeling or rules logic should look for high-velocity use of data points associated with many accounts. There are limits on effectiveness, however, considering what data points are being considered and how the quality of the data points is assessed. Phone numbers are more costly to create than email addresses, for example, but if an organization is not authenticating that a phone is associated with a name or address, users can continually provide phone numbers that do not belong to them when creating additional accounts.

Verification without first performing authentication is not nearly as valuable.

SMS text message verification can confirm a user is in possession of the phone number they provide, and is a sufficient check at the account creation stage—**with a critical caveat.** Verification without authentication is not nearly as valuable. In other words, you have confirmed that the user is in possession of the phone number but have done nothing to show that this phone number is connected to the name, address or other identity data points provided.

Link analysis checks can help with promo code, free trial, and referral abuse, and is something all organizations should consider at the account creation event. This begins with lower-cost checks leveraging existing user data, ramping up to potential identity checks when there appears to be some identity data that is being reused. For most organizations, referral abuse is going to be most costly and would justify more of a cost to mitigate. Free trial abuse is not relevant to as many organizations as promo abuse, but could be more costly for those who offer free trials.

When it comes to deciding when to perform step-up checks at account opening, identifying reused data points via link analysis is typically enough to warrant a closer look. Organizations should also consider the quality of data provided. If the BIN/IIN range (first 6 digits of a payment card number) indicates a prepaid or virtual card may be in use, or if the phone number is associated with a prepaid or VoIP phone, further screening may be worth the additive costs.

Consider how loyalty program policies and the timing of when reward points are provided impact exposure to loyalty fraud and abuse.

Defending against loyalty abuse can leverage link analysis to identify new accounts that use data points associated with past patterns of abuse, but much of this can also be reduced or eliminated through policies. Loyalty points should not be earned until the good or service is delivered, which can mean not until after a flight or hotel stay for a travel merchant or aggregator. There should also be a mechanism to automatically revoke loyalty points after a refund or chargeback.

Experienced loyalty abuse scammers may try to time their actions such that loyalty points are spent before or during the refund or chargeback process. The shipping address and other data points associated with these accounts should be put on negative or watch lists.

"Ekata has been instrumental in helping Bunking proactively fine-tune our fraud solution to safeguard marketplace trust and safety. With easily provided personal information, we're able to create different workflows based on risk profiles — eliminating any potential onboarding friction for good customers while protecting our community."

Ekata Customer — Darren Cody, Product Manager at Bunking

Guarding Against Hard Fraud

According to the Javelin 2022 Identity Fraud Study[2], new account fraud increased by **109** percent between 2020 and 2021. Wouldn't it be nice to nip these fraudulent accounts and associated potential losses in the bud? Reducing account opening fraud losses not only protects the bottom line, but also protects margins by finding and eliminating threats before they move on to credit screening and other more costly checks down the road.

With the help of the Identity Risk Score and other signals, Ekata helped a top food and beverage vendor catch fraudulent account sign-ups with 95 percent precision.

Challenges

Email harvesting often flies below the radar but presents challenges around brand risk as well as challenges on how to prevent it. At the account creation event, if you do not allow multiple accounts to use the same email address, there is no way to convey that an email is already in use without implying that it is already associated with your site or service. Mitigation tends to focus on bot prevention, but intentional harvesting can be manual or reduce the frequency of bot attempts to evade detection.

Email harvesting refers to bots or fraudsters that repeatedly attempt to create accounts to see if an account associated with an email already exists. If so, that account will likely be targeted with phishing attacks or account takeover.

Brand risks associated with this activity pose a significant challenge as customers can be targeted with sophisticated phishing campaigns that emulate an organization's brand, messaging and tone. Simply allowing users to create multiple accounts with the same email address is not an option for most organizations.

Preventing the **monetization of stolen identities** is also a challenge in that these attacks typically come from sophisticated fraudsters in possession of clean, or fully compromised, identities. Similarly, with **monetization of stolen payment credentials** there is potential for a meaningful fraud loss and step-up authentication screening techniques that increase both cost and friction can be warranted. The challenge is determining when these techniques should be applied, as using them across the board would be costly and diminish conversion or completion of new account setups.

Sources:
2 - https://www.paymentsjournal.com/19th-identity-fraud-study-shows-52-billion-in-losses-42-million-americans-affected/

When it comes to the monetization of any stolen PII, organizations should look at account opening as a precursor to the transaction event where the direct fraud loss ultimately occurs, but the greatest challenge is balancing when to apply various techniques to collect these risk signals while considering the cost, and potential friction, of doing so.

Risk Mitigation Techniques and Strategies for Hard Fraud

The primary strategies discussed around risk mitigation for soft fraud, link analysis and data quality checks, apply to hard fraud mitigation strategies as well. When concerned with or seeing signals of potential hard fraud, identity authentication and verification should also be considered. There is more allowance for friction based on the direct financial impact of missed fraud, but strategies should still focus on routing low-risk signal users to a “fast track” while those showing signals of higher risk see higher scrutiny, which entails both higher friction and higher costs.

Data Quality

A great place to start is extracting maximum value from the data points already collected from all new accounts with a focus on minimal friction and screening costs. Data quality checks provide a balance of low cost and low friction (zero additive friction if the data point is already being collected), but the costs tend to ramp up across the three levels of data quality checks that should be considered:

1. **Could the data point possibly exist?**
2. **Does the data point have history and credibility?**
3. **Has the data point been presented before across internal and/or external networks?**

This begins with data quality checks, such as whether the data point has the potential to exist, like a 555 area code. The second stage of data quality goes a step beyond to gauge the quality of the data point based on how easy or costly it is to acquire or present, in addition to other signals of its history or trustworthiness. This includes considering email domain risk, the age of an email and quality signals on the type of phone number, where postpaid mobile is favorable to prepaid mobile and VoIP lines.

Email domain, age of the email address and the type of phone line are second-level data quality checks that are low cost and low friction.

While the third level of data quality checks tends to have a higher cost than the previous two, these checks may provide a signal of risk that allows an organization to decline a new account or their eventual transaction and eliminate other risk screening costs that would otherwise occur along the way. **Data sharing** or network data checks apply link analysis techniques beyond the data points an organization possesses directly. Organizations can benefit from identifying user data points with high-volume activity across a third-party provider's network. It enables them to stop risky users even though it is the first time the merchant, app, or site has seen those data points. Cross-merchant or organization velocity checks, beyond just shared negative lists, provide a lot of value leveraging data points that are already collected during account creation.

Authentication & Verification

The next layer will focus on more automated screening, which potentially requires higher costs to perform. This may include authenticating and verifying identity data points to see that, beyond their quality, there is association and ownership of the data points provided.

Both potential friction and financial costs need to be considered, but the next determination is whether or not the third layer is required. Third layer screening may include manual review and other higher cost or higher friction techniques reserved for orders that cannot yet be accepted or declined with confidence. Following the post–data quality automated screening, users can be fast-tracked if they have only shown signs of low risk or moved to higher-cost third-layer screening such as manual reviews or knowledge-based assessments (KBAs).

In the lending space, credit checks will be a fourth layer, where the manual review or KBAs may be skipped on the fast-track, or the credit checks may not occur based on the outcome of manual reviews and KBAs. While manual reviews and KBAs are costly, credit checks are typically the most expensive and should be reserved for the final steps of the onboarding workflow.

In the goods and services space, screening beyond the second layer is typically reserved for when the user attempts their first transaction. This balances the value of collecting data points along the way with paying for checks that utilize them when they are more needed. Many signals can be recorded during account creation that will later provide value, so it is generally better to collect data and not need it than want it but not have it.

There are many considerations around **sleeper accounts** in this regard as well. Merchants need to consider how they measure user account trust and how that impacts risk models or rules engines as a positive risk signal. Looking solely at account age can be misleading; account activity is a more valuable signal. Fraudsters may create user accounts and wait months to use them, but if that account has had no purchase activity since inception, it should not be viewed any more favorably than a guest checkout.

It is best to think of the account opening risk mitigation strategy as a layered approach that increases in cost, and potentially friction, as users move through the process while considering the perceived risk from data points collected along the way. The first layer focuses on data quality checks from the data points already collected. But from there, the path can split several different directions and things get more complicated.

Third-Party Vendor Considerations

Many risk management checks and considerations come together as users create their account or complete an application. From initial data quality checks to additional layers of screening, multiple third-party solution providers likely come into play alongside in-house screening techniques and internal data. Considerations for layering techniques provided by third-party vendors, along with how and when to apply them, is the final topic concluding this white paper.

Breadth of Network Data

Thinking back to discussions around data sharing, breadth of the data network is important. The larger the data network, the more likely it is that personal identity information will be recognized — even when it's only been previously used outside your organization. This is not something an organization can easily build in-house, as the value of network data comes from shared velocities, shared negative lists, and other data aggregated across a data vendor's client network. With this in mind, the more clients a vendor has participating in their data sharing pool, the more likely it is that any one client will get a hit on a data point seen previously by others but not by their organization directly.

Breadth of network impacts how likely it is that data points frequently provided by fraudsters will be detected across shared velocities and negative lists.

Ability to Tackle Different Types of Fraud

Risk vendors with a focus on soft fraud are less prevalent in the market. From the nascent days of eCommerce until only several years ago, fraud prevention focused on hard fraud with little-to-no consideration for peripheral or soft fraud schemes. If an organization is intent on curbing promo abuse—including free trials and referrals—finding a service provider with experience in these areas can be a key part of their value proposition.

In short, if detecting and mitigating soft fraud risks is important to an organization, they should seek out solution partners with experience and expertise in this area. Ask vendors about the aspects of their service that are applicable to soft fraud signals and about the success they have seen in helping their clients reduce different forms of abuse.

Place in Overall Risk Strategy

Lastly, where does the vendor or service fit within your risk strategy? Is it the first, second, or third layer or beyond? Is it automated or intended for manual processes? These considerations are directly related to the cost of the service and the potential friction it presents, with both factors dictating how early or late in the user flow, and how often, you intend to call out to this service provider.

Vendor consideration must be grounded in what the organization is looking for: point tools, a platform, or both. There are platform providers that serve as the backbone of risk architecture, which is important for digesting risk signals to make decisions and routing new accounts or orders through the layers of risk screening. This facilitates the outcomes, but not necessarily the data and risk signals that drive those outcomes. Therefore, organizations must also consider the many point tools and techniques that derive signals, such as various data quality checks, authentication, verification and other techniques. Some of these may be available within the same platform that provides the risk architecture, but many may not.

Early risk screening at the account opening stage will improve the detection and prevention of both hard fraud and soft fraud or abuse.

When considering the overall risk strategy, there is a tendency for merchants to focus on the transaction event and where the direct financial losses ultimately take place, but it is critical to capture the value from risk signals that can be derived from the beginning of the customer journey as well. While identity data can be leveraged across multiple stages, there is value in solutions designed with onboarding or account opening events specifically in mind. However, these solution providers are not as common in the marketplace.

Conclusion

Effective risk management must defend against both hard fraud and soft fraud like promo abuse. This is a challenge as most experienced industry professionals naturally put more focus on hard fraud and there are fewer vendors who support tools or services with soft fraud in mind.

Earlier detection of fraud and abuse, as well as low risk, enables more balanced and cost-effective fraud strategies by saving operational and vendor costs related to users or transactions that can be fast-tracked or declined sooner rather than later.

Organizations looking for the next area of improvement or who want to get ahead of where fraud is trending would do well to assess their risk management strategy with an increased focus on soft fraud and abuse. It may seem like a large undertaking to add abuse detection and prevention to a risk management strategy, but strategies already built with a layered approach are well positioned to add soft fraud risk signals.

Similarly, starting from a point of no visibility into soft fraud, making a risk strategy more robust with a focus on detecting promo abuse and its many forms may seem costly. Taking a layered approach that applies lower-cost data quality checks first, weeding out bad accounts and fast tracking the best ones, can be cost effective when considering the operational and third-party vendor costs saved through effective routing or new users and applicants.

If “an ounce of prevention is worth a pound of the cure,” as Benjamin Franklin so wisely said, then implementing fraud prevention earlier and more often can be even more valuable.

About the Fraud Practice

The Fraud Practice is a privately held company based in Palm Harbor, Florida. The Fraud Practice provides training, research, and consulting services on eCommerce payments, fraud prevention, and credit granting. Businesses throughout the world rely on The Fraud Practice to help them build and manage their fraud and risk prevention strategies.

For more information about The Fraud Practice's consulting services, please visit www.fraudpractice.com. For additional information about The Fraud Practice's online training programs, please visit www.CNPtraining.com.

The Fraud Practice
www.fraudpractice.com
www.CNPtraining.com
Telephone: 1.941.244.5361
Email: Questions@fraudpractice.com

Are you looking for answers or solutions, for eCommerce payments and fraud management? Give us a call for a free introductory consultation to see if we can help you. Even if we can't meet your needs we most likely know someone who can, and we are happy to provide you with contacts of reputable firms and individuals servicing the space.

David Montague,
Founder

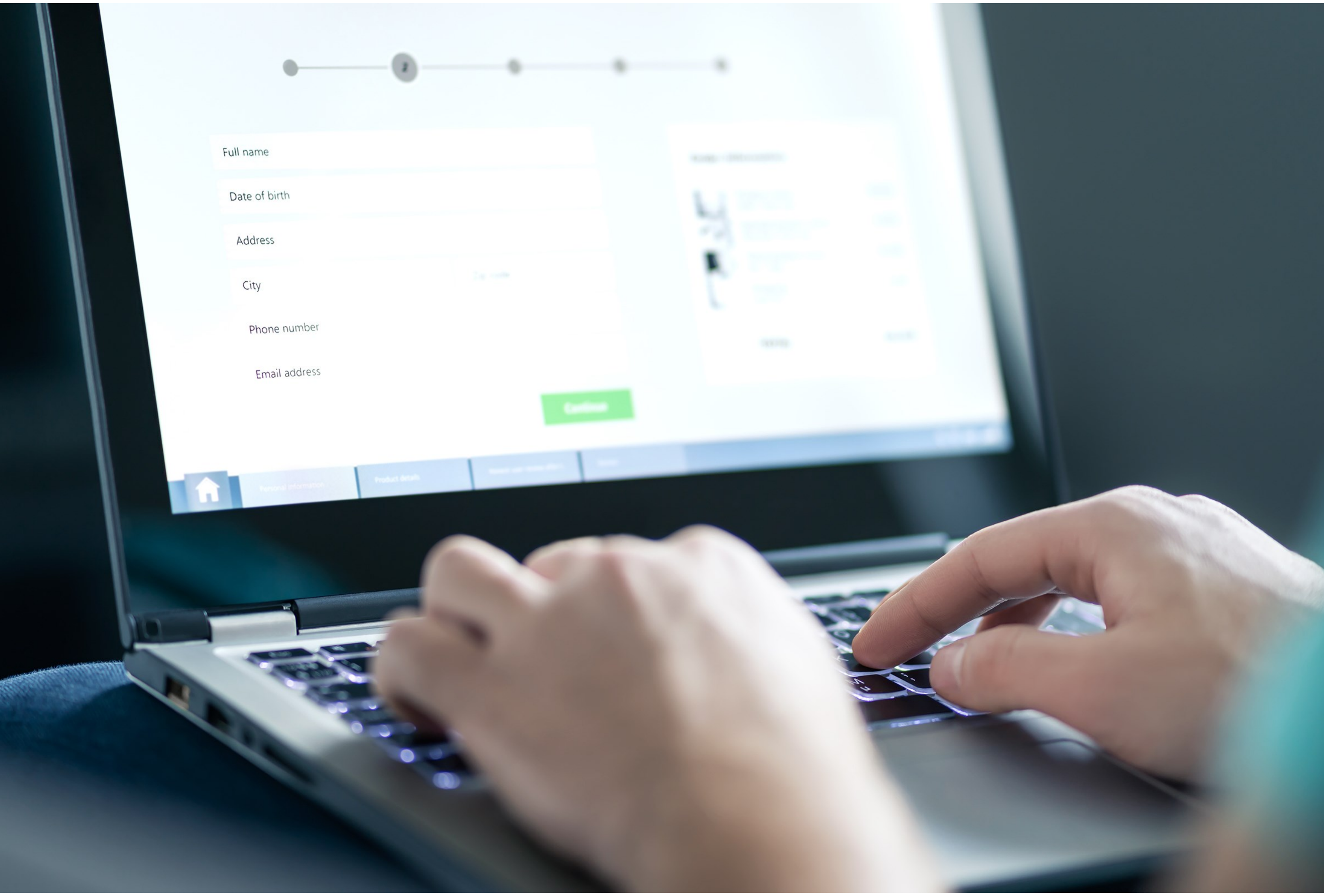
About Ekata

Ekata Inc., a Mastercard company, empowers businesses to enable frictionless experiences and combat fraud worldwide. Our identity verification solutions are powered by the Ekata Identity Engine, which combines sophisticated data science and machine learning to help businesses make quick and accurate risk decisions about their customers. Using Ekata's solutions, businesses can validate customers' identities and assess risk seamlessly and securely while preserving privacy. Our solutions empower more than 2,000 businesses and partners to combat cyberfraud and enable an inclusive, frictionless experience for customers in over 230 countries and territories.

Contact us to learn more.

www.ekata.com | 1.888.308.2549

THEFRAUDPRACTICE
PROTECTING THE BOTTOMLINE



IS THIS *REALLY* A NEW USER? DETECTING FRAUD AND ABUSE AT ACCOUNT OPENING

White paper by The Fraud Practice
Sponsored by Ekata, a Mastercard Company