WHITE PAPER

Mitek

Fraud trends and tectonics

Financial services and online marketplaces both face rapidly shifting fraud landscapes – and can learn from each other.

Sanjay Gupta, VP product management, Mitek

In the digital age, fraud—always requiring the attention of financial services and online marketplaces—has become a stronger force of potential business upheaval. Over the past couple of years, we've seen high double-digit or even triple-digit rates of increase in digital/online payment fraud and account takeover fraud. Synthetic identity fraud is the fastest growing financial crime in the US. There's also fear that deepfakes could wreak havoc across the entire fraud landscape.

These are signs that the foundations of traditional fraud management are fracturing. Pressure is building for a serious 'fraud earthquake.' And all are heightened by the dramatically accelerated movement to digital channels due to the pandemic.

What can you do to navigate this shifting ground and avoid potentially tectonic shocks to your business? A key to success is understanding the interrelationship between identity, fraud and trust. In this report, we look at how it plays out in financial services and online marketplaces. We find that companies in both industries can better defend their customers, platforms, brand reputations and financial stability if they learn from each other's experiences and best practices.

May, 2020

Why is the ground moving?

Like many of you over the last few months, I am working at home: Zoom meetings on my laptop, kids running around in the background, and most days my work uniform includes sweatpants. And while my colleagues and I were trying to create schedules in 'the new WFH normal,' you can imagine how surprised we were after a 4.9 earthquake hit San Diego county where Mitek is based.

Fortunately, it was small enough that we didn't experience damage. But it was scary. I thought "Great - I don't just have to worry about a pandemic anymore, I have to think about earthquakes too!" I started to rethink my preparedness, get supplies together, and plan for a worse one in the future.

We forget that earthquakes don't just affect the real world. Online, there's digital earthquakes caused by fraud everyday. But the "ground" in fraud management used to be more stable. Digital companies I work with in financial services and online marketplaces have necessarily accepted some level of fraud losses as a foundational cost of doing business.

Current trends are leading to more frequent fraud earthquakes. Though we might not feel them now, bigger ones are coming. For instance, Juniper Research reports online payment fraud for businesses in eCommerce, banking services, money transfer and airline ticketing jumped from $26 billion in 2018 to nearly $50 billion in 2019. At that rate, we're looking at some $200 billion in cumulative fraud losses between 2020 and 2024.

Worst year for data breaches

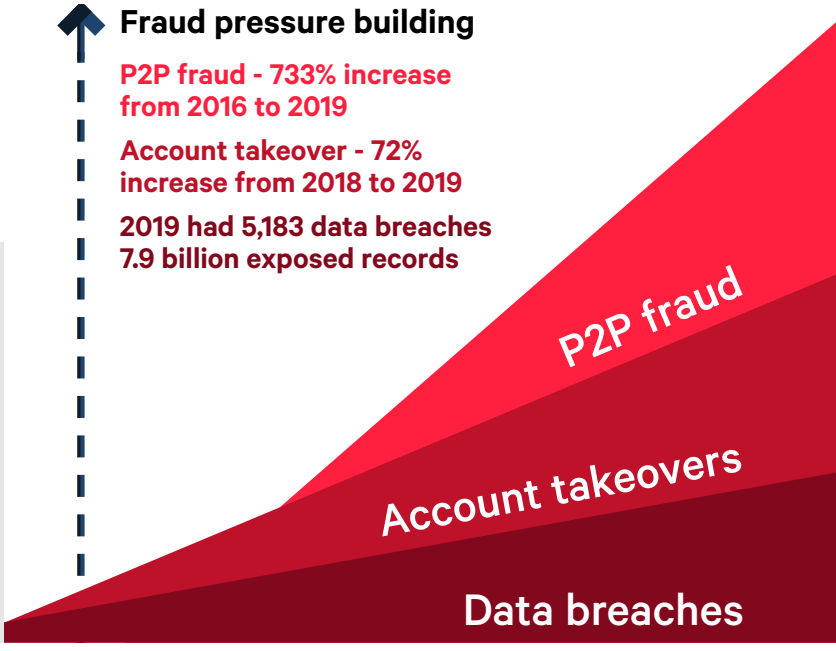
Data breaches fueling rising fraud levels continued to occur all over the economic map in 2019—the "worst year on record" according to research by Risk Based Security. The CNET "Data Breach Hall of Shame" for last year included financial services companies American Financial Corp and Capital One as well as online marketplaces MoviePass and DoorDash.

The full financial damage may be even greater than we notice. Some studies suggest that for every dollar online merchants lose to fraud, they absorb three times that amount in chargebacks, merchandise replacement and other related expenses. For financial services, it's been estimated fraud accounts for more than 20% of credit losses, and up to 10% of bad debts may actually be fraud masquerading as delinquencies. And since these estimates are based on studies now several years old, today's percentages are likely considerably higher.

What's causing this strong movement in fraud trends? Proliferation of digital channels and accounts, massive data breaches and advanced technology like AI are all contributing factors.

With easy access to abundant consumer data, computational power and tools, fraudsters are compromising or completely taking over legitimate accounts. Moving fast, they often start inflicting monetary damage within a day of the intrusion.

At the same time, some fraudsters are expanding into more complex, patient schemes aiming for larger payoffs. They look and act like legitimate customers until the moment they strike big.



Sources: Data breach and exposed records - CNET; ATO and P2P data - Javelin.

Identity, fraud and trust

Another reason for rapidly rising fraud trends is that online marketplaces and financial services, including fintechs, have largely employed defenses called 'point solutions'.

Point solutions at a bank: Traditionally banks have verified identity at account origination, then run analytic fraud detection on customer transactional patterns. Different groups within different lines of business "silos" have been in charge of these methods, with little information sharing between them.

Point solutions have evolved with digital: Many fintechs and online marketplaces, intent on rapid customer onboarding to drive growth, have minimized identity verification at account origination. They've accepted identities from other digital platforms and services, perhaps running some background authentication processes. More explicit identity verification is only invoked if unusual transactional patterns indicate fraud or if dormant accounts suddenly become active.

The effectiveness of these defenses is diminishing as digital identity becomes the master key criminals use to open doors. Point solutions are often partially blind to schemes that cross lines of business and come into play months after a false identity was used to open a new account. They may not be quick enough spotting fraud when a trusted account suddenly starts behaving in uncharacteristic ways.

Today's defenses need to be built understanding both identity and fraud are intertwined throughout the customer journey. Financial services and online marketplaces likely know how this interrelationship affects customer trust, but do they know that consumers don't mind friction if it means better security?

Recent studies show that many consumers feel greater trust in online platforms and services if their identities have been verified at onboarding. When that step is missing or too lightweight, consumers may feel less trust.

Consumers also want to be recognized when they return to transact. In fact, according to Experian research, they "trust businesses most when they feel recognized."

Here's where the balance between low friction and high security is critical. On one hand, consumers don't want to be put through frequent identity reproofing (or at least they don't want to be aware reproofing is going on). On the other hand, if an account breach or takeover occurs, the potential impact goes beyond monetary harm and hassle. Customers are likely to feel a deep sense of insecurity about doing further business, and decide they now have evidence the company really doesn't know who they are and that they don't care.

79% **of consumers are concerned about data security when using connected devices to enable a payment —** an 11% increase of the year before

PYMTS and Visa survey, 2019

74% **of consumers say security is the most important element of their online experience —** above convenience

Experian 2019 Global Identity and Fraud Report

95% of businesses claim they can accurately identify their customers;

55% **of consumers disagree**

Experian 2020 Global Identity and Fraud Report

How fraudsters are leveraging identity

A trusted identity is a valuable thing, and fraudsters know it. An increasing amount of the fraud and abuse being seen by financial services and online marketplaces revolves around identities.

Some of it is **first-party**. The perpetrator owns the identity but is leveraging it, or allowing someone else to leverage it, for financial gain.

In an online marketplaces

there might be a rideshare driver illegally subcontracting work to others, underpaying them and pocketing the difference. This can be a serious threat to the integrity of the marketplace and customer trust.

In financial services

there might be customers listing potential fraudsters as secondary account holders, thereby enabling them to benefit from the customer's credit history. This widespread practice called 'tradeline selling' is a source of considerable losses. For example: a borrower with bad or zero credit history piggybacks off a verified user to get a better credit score in order to secure a low interest rate on a loan. The borrower would save tens of thousands in interest payments, meaning losses on potential profits for an issuer.

While these problems are serious, the most alarming growth in identity-related fraud is third-party. That's where the perpetrator is not who they say they are. This type of fraud is occurring in both new accounts and takeovers of existing accounts.

Let's see how fraud is playing out in financial services and online marketplaces...

2020 FRAUD TRENDS IN FOCUS

Synthetic identities

Account takeover

Fake accounts

Source: Mitek poll administered in March 2020 to participants in Mitek's "Identity Innovator series."
Poll Question: "What fraud trends have you been watching over the last 6 months?"

New account fraud

According to NuData, **one in five new accounts in 2019 were likely fraudulent**. New account fraud is rising partly because there's now a low-risk, high-payoff way of doing it--synthetic identities. A report by the Federal Reserve Bank cites research (McKinsey) showing synthetic identity fraud is the fastest growing type of financial crime in the US.

Traditionally, fraudsters have used their own or stolen identities to open new credit or service accounts. They'll transact as much as possible as soon as possible before a delinquency is flagged as fraud. Oftentimes this happens before an identity owner becomes aware of the unauthorized account.

Today fraudsters are increasingly using synthetic identities to open new accounts. Sometimes these identities are entirely fake. More often they're a unique assembly of a) made-up information, b) stolen real or slightly modified personal identifying information (PII) hacked from databases or c) bought dirt-cheap on the dark web.

This type of crime usually has a limited initial impact on the individuals whose PII is being used, so the problem may go unnoticed for a while. Also, because synthetic identities look legitimate at onboarding and fraudsters manage the newly opened accounts to mimic legitimate user behavior, fraud defenses may not pick them up. That gives fraudsters time to spin out complicated schemes for stealing funds, purchasing high-value goods or making money illegally. And, of course, synthetic identities not caught by Know Your Customer (KYC) requirements may also play a part in large-scale money laundering schemes.

New account fraud in financial services

According to GIACT, 85-95% of fraud from synthetic identities are not caught by the models used at account opening to predict third-party fraud. Fraudsters that get through bide their time, earning higher levels of credit or services and possibly lower levels of security with their normal purchasing patterns. At the moment of maximum advantage, the fraudsters "bust out" to take as much as possible, then disappear. The result is large write-offs of unpaid debt. In fact, McKinsey estimates that 10-15% of losses in a typical unsecured lending portfolio are the result of fraud perpetrated through synthetic identities.

New account fraud in online marketplaces

Synthetic identities are being used to purchase goods or services using stolen payment cards or person to person (P2P) accounts. Opening accounts for dozens of nonexistent individuals, fraudsters will take advantage of new customer promotions or "refer a friend" offers. On the sell-side, fraud is often aimed at selling counterfeit products. A marketplace version of bust-out fraud could involve a seller legitimately fulfilling orders for authentic products long enough to earn high customer ratings, before suddenly filling the order pipeline with counterfeit versions. Or the fraudster might accept a large number of orders, stop fulfilling them and just disappear.

Strengthening your defenses against new account fraud

Always consider and evaluate the information you receive.

We advise companies to reduce reliance on static PII, such as social security numbers, at account origination. Also don't give too much weight, from a fraud detection perspective, to credit bureau information.

Financial services typically check credit bureaus when someone applies for an account. If there's no credit file for that identity, the application will probably be rejected by the financial service. Meanwhile, as a result of the inquiry, the credit bureau has created a "thin file" (because it doesn't contain much information). In normal practice, this helps someone like a young person or recent immigrant trying build credit. As an unintended consequence, the next time the fraudster tries to open an account with that synthetic identity, it will match to the thin file, looking like a legitimate consumer. Fraudsters understand and regularly exploit this -- that's why a common method is to apply for accounts across lots of different companies.

Many fintechs and online marketplaces avoid this problem by analyzing a wider range of data at onboarding. The mix might include demographic and publicly available information like property records, online purchases, social media activity, and device and geo-location data. The idea is to assess whether an applicant's "context" has the depth, breadth and complexity characteristic of a real person. Still, caution is called for, since not all sources verify their data. Also, sophisticated fraudsters have the tools to spoof device and geo-location data. They often invest a considerable amount of time and effort shoring up valuable synthetic identities by engaging in online activity and creating convincing presences on social networks.

Help applicants put their real face forward.

With so much PII floating around, many companies are turning to biometrics, such as facial authentication, for verifying identities at onboarding. For instance, online and mobile software can guide applicants to quickly prove their identities by submitting a snapshot of a government-issued ID along with a selfie. In a few seconds, AI algorithms analyze and compare the submissions, determining if the document is authentic (not counterfeit or altered), if the selfie is a live person (not a photograph, video, or even a masked individual), and if they match (same individual in both selfie and document picture). This kind of defense is effective against synthetic identities since most fraudsters don't want to use their own faces, and faking a face still involves a lot of work (see sidebar on biometrics and deepfakes).

Ask yourself 'where have we seen this before?'

Another helpful defense against synthetic identities at account opening is link analysis. Because fraudsters frequently reuse pieces of PII, software that looks for these overlaps can quickly highlight suspicious identities. It can find, for example, phone numbers or addresses that have been used for other identities, including those associated with fraud or members of suspected fraud rings. Fuzzy logic enables link analysis to pick up near matches, where fraudsters have made minor alterations to real PII.

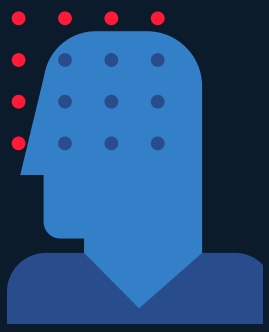
Adopt new models for a new era.

Traditional analytic models aren't effective against fraud perpetrated through synthetic identities. This includes the application fraud models many financial services use at account origination and the behavioral models they rely on to pick up signals of impending fraud in early-life accounts. The problem is that the accounts of synthetic identities often look quite similar to those of legitimate identities at onboarding and after.

Also, we're just starting to compile enough cases of confirmed fraud via synthetic identity for data scientists to identify customer characteristics that may be predictive for building and training more effective models. Some companies, for instance, say they've been able to isolate applicant behaviors at the time of account opening that may correlate with high credit activity when synthetic identities begin to execute bust-out fraud. A McKinsey demonstration, working with 15,000 profiles from a third-party consumer marketing database (while adhering to data privacy regulations), was also encouraging; by identifying and analyzing 150 customer characteristics, McKinsey was able to focus in on the 5% of profiles most risky for synthetic identities.

These types of analyses could help financial services and online marketplaces selectively decide when to invoke more stringent identity verification at onboarding.

BIOMETRICS BREACHES AND DEEPFAKES



Physical biometric authentication has certainly heightened the wall of fraud defense, but it's not unassailable. In 2019, we saw the first biometric database breach, which fortunately was the work of white hat security researchers.

Additional breaches by less sympathetic actors are expected in the near future. Widespread adoption of biometric authentication is creating more biometric data stores, not all as secure as they should be. Meanwhile over the past year, a hot market for this kind of data has emerged on the dark web. Most of what's currently for sale is facial biometrics from selfies and videos fraudsters are harvesting from social media or obtaining through phishing schemes.

Biometric data is in demand partly because it can be used with AI algorithms to create deepfakes that look and sound like real people. Deepfakes have so far been used mostly for celebrity-bating, political dirty tricks, pornography and one notorious case of corporate extortion. As the technology improves and becomes commoditized, however, it could be used for identity-theft crimes, including fraudulent account opening and account takeover.

To counter this threat, it's important to make sure facial authentication software includes certified liveness detection. And because sophisticated deepfakes can spoof common movements like blinks and nods, authentication processes will need to evolve to guide users through a less predictable range of live actions.

Account takeover fraud

A new report from Javelin Strategy & Research says **account takeover fraud (ATO) rose by 72% from 2018 to 2019**. One reason ATO is surging is because it is easy for fraudsters to intrude on an existing account than to open a new one. The potential rewards may be greater, the payoff quicker and—because an established, trusted relationship might be subject to minimal fraud controls—the risks lower.

Why has ATO become so easy?

For one thing, there's an abundance of targets, with many consumers having a dozen or more accounts. Some of these may be dormant. DataVisor says 65% of ATO attacks are on accounts that have been inactive for 90 or more days. There's also an increasing number of digital channels into these accounts; recent Aite Group research shows that many banks have seen digital channel usage increase 250% in the wake of the pandemic.

The constant data breaches fueling synthetic identities for new account fraud are also fueling ATOs. Consumers, of course, continue to make personal information available via social media. Many are tricked into revealing it through phishing schemes, social engineering and other scams—dramatically on the rise under pandemic conditions. And despite warnings, many account holders still use the same passwords across multiple accounts. As a result, brute force attacks, using bot farms and other automated tools to try login pairs across numerous accounts and platforms are still effective.

Once fraudsters have access to an account, they will usually attempt to change account details, such as phone number and address, as an enabler for perpetrating all kinds of crimes.

In financial services

ATOs enable fraudsters to use the account holder's credit by making online purchases via a payment card or even applying for a new loan or line of credit. Fraudsters might also make P2P payments to themselves or collaborators.

Fraudsters sell credentials for accessing compromised accounts. On dark web sites, accounts with higher credit lines and credit scores fetch better prices. In fact, to put the right price tag on an account, some fraudsters even use the same types of fraud detection analytics traditionally employed by banks; accounts with characteristics (like purchasing behavior patterns or router locations) that fraud models see as riskier will be cheaper on the dark web.

The results for financial services are largely seen in charge-backs for transactions challenged by legitimate customers. On top of that is damage to customer experience and trusted brand reputation.

In online marketplaces

ATOs enable sell-side fraudsters to subvert legitimate vendor listings, substituting counterfeit products or just taking orders without delivering products. On the buy-side, fraudsters can tap the account holder's loyalty points for rewards. If payment methods are stored in the account data, they can sign up for premium digital services, make fraudulent purchases and book rentals or entire vacation packages. There are dark web sites where fraudsters post photos of fraudulently obtained hotel rooms and offer multipacks of compromised accounts for online gaming and music/movie streaming, priced according to subscription levels and quality of the original accountholder identity's credentials (location, credit score, potential fraud risk, etc.).

The results of sell-side ATO include the cost of replacing counterfeit or unfulfilled goods. For buy-side ATO, marketplaces have to relay charge-back requests on disputed purchases to payment card processing companies—too many of these and processing fees go up. In all cases, there's negative impact on customer experience and trust.

Strengthening your defenses against account takeover fraud

Practice basic security hygiene.

These include not relying on username/passwords and knowledge-based authentication. Above that, activate layers of security based on the risk level of the activity.

Use physical biometrics where you can.

If fingerprint, voice or facial data was captured at onboarding, these biometric checks provide a strong extra layer of security for ongoing access and protection against ATO. Still, physical biometrics are not the "silver bullet" they were once thought to be, as biometric data has been hacked and has begun to appear for sale on dark web sites.

Expand user profiling for passive checks.

Most companies employ some mix of passive methods to authenticate returning customers. Often these include checking device data and geo-location against a user's profile. But with fraudsters able to easily spoof such checks, profiling is expanding to capture a growing variety of user data. Behavioral biometrics, such as how account holders tap their devices and navigate through web pages, are being used to compare what users are doing in real time with what they've typically done in the past. This approach is not useful for dormant accounts, however, since data on account activity will be scarce or stale.

Get help from fast learners.

Machine learning (ML) can be used in conjunction with or in place of analytics to spot unusual behavior indicative of fraud risk. This type of AI (artificial intelligence)—often called "unsupervised" because it's not trained on historical data—analyzes and rapidly learns from current data. As the data streaming in from user transactions changes, some ML models continually recalibrate ranges of normal behavior for users with similar characteristics, and spot outliers to these dynamic ranges.

Go active when you must.

For high-risk/high-value transactions such as money transfers or attempts to change account details, passive methods can be combined with active methods. These might include two-factor authentication using a one-time token or confirmation via an alternate channel, like SMS, that it's the legitimate user making a change or transaction.

In addition, account holders' identities may need to be reverified at various moments during the customer journey. Indeed, some companies routinely invoke identity verification whenever a dormant account suddenly becomes active, for high-value transactions or when passive analytics indicate elevated fraud risk.

One way to do this is to request a current selfie, then compare it to the biometric data stored from onboarding (where storage is allowed by regulations and permissioned by the customer). In very risky situations, you could also request a new snapshot of the originally submitted government-issued physical ID, and take a few seconds to verify the authenticity of the document and compare the photo on the ID against the selfie. Indeed, there is an emerging trend among identity leaders to think of identity verification as something that extends beyond onboarding and risky transactions. This new approach threads identity awareness through the customer journey, placing a verification "stitch" at certain points. These stitches might be at specified periodic intervals. They could be triggered by a specific event or even randomly invoked, making it difficult for fraudsters to anticipate and circumvent the added security measure.

The AI wars

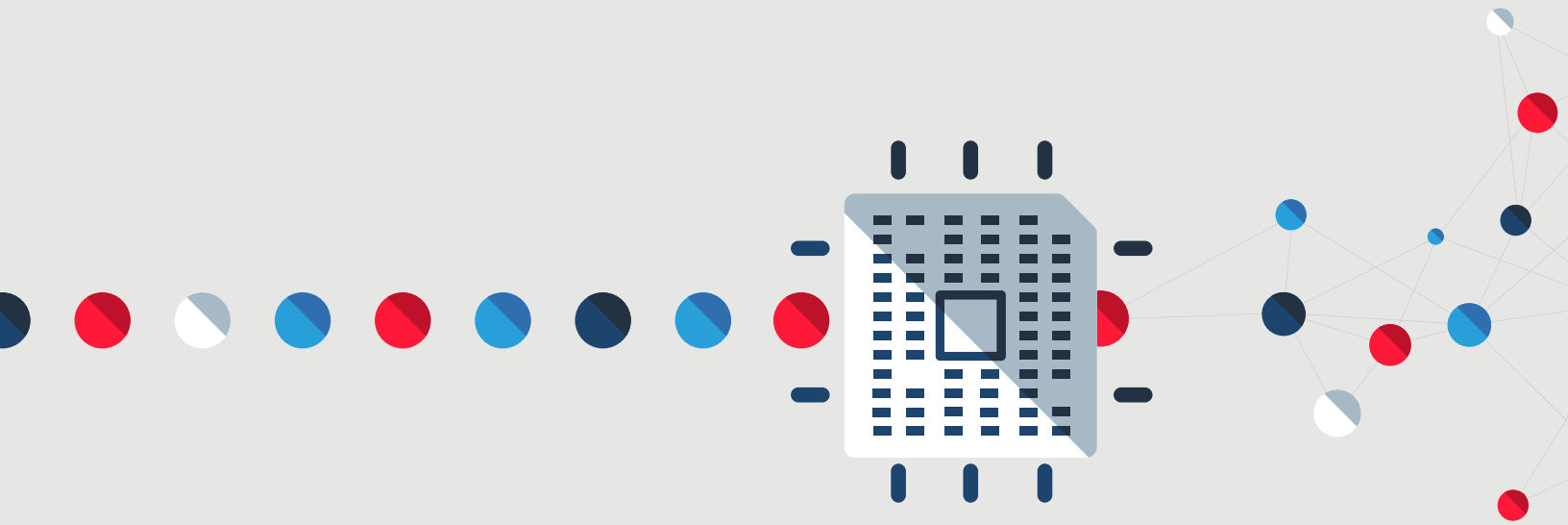
We've talked about how financial services and online marketplaces are using machine learning to try to tell the difference between the typical behaviors of legitimate customers and fraudsters. **The problem is that fraudsters have access to the same AI technology, and they're using it to get better and better at imitating normal behavior.**

Last year Kaspersky Lab, an anti-malware software company, revealed it had discovered a dark web marketplace with vendors offering over 60,000 packs of login credentials accompanied by "digital masks." The masks were built by machine learning algorithms that analyzed online and device behavioral patterns of consumers whose PII had been compromised. Using the stolen login with the mask from a proxy browser, fraudsters have a better chance of thwarting fraud detection and taking over an account.

This is an example of how fast technology, and adoption of it, are evolving. For this reason, no one approach is ever likely to provide complete security, and a mix of security methods is recommended.

Today, fraud protection is increasingly about using AI to "connect the dots" between different types of consumer data to get a picture of whether or not the customer is legitimate.

Identity-related fraud crimes are increasingly about using AI to know where to "place the dots" to create a picture that looks legitimate.



"Kaspersky Lab Unearths Dark Web e-Shop that Sells Stolen Digital Identities," FindBiometrics
"Kaspersky Lab Uncovers Genesis: The Underground E-Shop with Tens of Thousands of Digital Identities," businesswire April 9,2019

Best of both

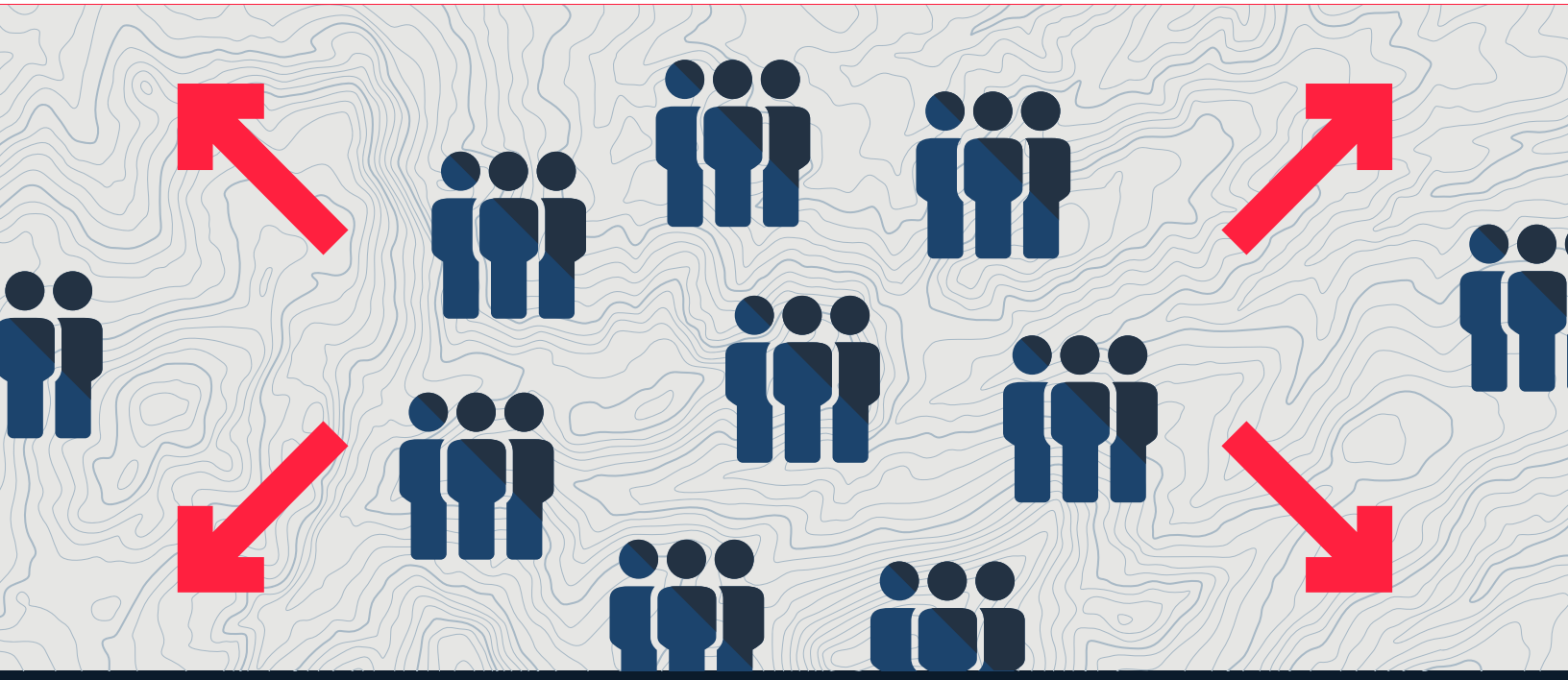
Financial services and online marketplaces both have strengths when it comes to fighting fraud.

FINANCIAL SERVICES		ONLINE MARKETPLACES
Do well Traditional banks have strong fraud teams with well-established procedures for investigating suspicious transactions, communicating with customers and processing chargebacks. Fintechs may be organized differently, but still have fraud management experts.	→	**Can learn** Fraud management may be tucked under platform security or assigned to the group responsible for customer experience. For better control, break out focused fraud teams, while retaining communication and collaboration between all these functions.
Can learn Separate operations for lines of business and functions such as account origination and customer management have created siloed systems/data that impede fraud visibility and defenses. Companies can rise above silos with new technologies that access and combine data from multiple internal and external sources.	←	**Do well** Digital-first organizations like online marketplaces and fintechs have set up their operations to support seamless customer journeys across an expanding array of products and lines of business. That gives them good visibility into varied fraud attempts and complex multi-step schemes.
Do well Established financial services have rich troves of customer transactional and other behavioral data. They've leveraged this data for fraud detection, and are gaining additional value from machine learning to spot morphing fraud schemes.	→	**Can learn** As marketplaces build up customer historical data, their modeling teams can borrow well-proven fraud detection technologies, such as adaptive models that self-adjust based on the disposition of suspected fraud cases.
Can learn Traditional financial services need to do more with alternative data sources so they can reduce reliance on credit bureau data and static information like social security numbers.	←	**Do well** Online marketplaces and fintechs are adept at combining and analyzing different types/sources of data for expanded views into the behavior of legitimate customers vs. fraudsters.
Can learn Many financial services are also getting pretty good at self-service, but others still trying need to catch up with online retailers and fintechs.	←	**Do well** They're also great at customer self-service and communications, including multi-channel ways to check suspicious transactions.
Do well Regulatory compliance has long been a core competency of financial services. Most have compliance officers/teams who work with customer lifecycle functions, from onboarding through collections, to ensure adherence and manage reporting.	→	**Can learn** Many online marketplaces do not have people responsible for compliance. While not yet subject to Know Your Customer regulations, marketplaces should begin building capabilities, especially as there's a strong link between online fraud and money laundering.
Can learn Financial services have allowed months or years to elapse between software updates, and can be reluctant to recieve advice from partners. That's changing with new standards-based technologies replacing legacy systems with capabilities like callable services or adding new, innovative partners.	←	**Do well** Online marketplaces and fintechs are agile, some doing core updates to apps weekly or daily, and refreshing tech infrastructures every six months. Knowing when to build/buy, they work well with vendor partners. This approach supports rapid learning for finding balance points between high security and low friction in customer experience.

Pandemic acceleration

The shift to digital was already well underway, creating convenience and choice for consumers, opportunities for businesses—and an ever-expanding terrain for online and mobile fraud. Under Covid-19 this shift is accelerating dramatically, and so is the potential for fraud.

As more people move into the digital world, the terrain for fraudsters is rapidly expanding



Since start of the pandemic

World Health Organization (WHO) recommends consumers pay with contactless methods

Financial Action Task Force (FATF) encourages the "fullest use of digital customer onboarding and delivery of digital financial services in light of social distancing measures"

73% of consumers doing more remote work or errands; 63% more inclined to try a new digital app or website (Lightico survey)

Office of Personnel Management advises federal agencies to virtually or remotely onboard new employees

Goode Intelligence predicts 15-20% increase in digital identity verification in 2020

The $2 trillion Coronavius Relief Package recently passed is the perfect place for fraudsters to steal from. Neil Barofsky, previously the Special Inspector General of TARP in 2008, projects that up to $200 Billion could be lost to fraud.

Let’s get this right

Digital transformation trends that have been building for some time—shifting how we pay our bills, manage our finances, shop, work and play—are now markedly accelerating.

So is growth in the intertwined crimes of identity theft and fraud. They’re growing so fast they threaten the foundational trust consumers need to have in the digital platforms and services that are becoming the fabric of our lives. And what has until now been considered a necessary cost of doing business could become unsustainable.

You can’t predict an earthquake, but you can prepare for them. To avoid this potential upheaval to digital transformation and the benefits it brings, businesses are beginning to adopt a unified approach to identity verification and fraud management. Point solutions are being expanded into comprehensive defenses across customer journeys.

Financial services and online marketplaces, at the forefront of digital transformation, are prime targets for intensified fraud. Both have key pieces of evolving solutions for countering the rising threat—the rest, they can learn from each other.

Tell us what you think.

Share your ideas, observations and experiences here.

Mitek

Bibliography

McKenna, F. (2020, February 26). Online Fraud Will Cause $200 Billion in Losses in 4 Year [blog post]. Retrieved from https://frankonfraud.com/fraud-reporting/online-fraud-will-cause-200-billion-in-losses-in-4-years/

Juniper Research. (2020, February 25). Online Payment Fraud Losses to Exceed $200 Billion Over Next 5 Years [press release]. Retrieved from https://www.juniperresearch.com/press/press-releases/online-payment-fraud-losses-to-exceed-200-billion

Daly, J. (2020, April 7). The Fallout From ID Fraud And Account Takeovers Includes a Lot More P2P Payment Fraud. Digital Transactions. Retrieved from https://www.digitaltransactions.net/the-fallout-from-id-fraud-and-account-takeovers-includes-a-lot-more-p2p-payment-fraud/

Javelin Strategy & Research. (2020, April 7). Identity Fraud Losses Increase 15 Percent as Consumer Out-of-Pocket Costs More Than Double, According to 2020 Identity Fraud Report [press release]. Retrieved from https://www.javelinstrategy.com/press-release/identity-fraud-losses-increase-15-percent-consumer-out-pocket-costs-more-double

The Federal Reserve. (2019, July). Synthetic Identity Fraud in the U.S. Payment System. Retrieved from https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf

McKinsey & Company. (2019, January). Fighting Back Against Synthetic Identity Fraud. Retrieved from https://www.mckinsey.com/business-functions/risk/our-insights/fighting-back-against-synthetic-identity-fraud

PYMTS.com. (2018, December 24). 12 Ways Consumers Will Pay (And Be Paid) In 2019 And Beyond [blog post]. Retrieved from https://www.pymnts.com/news/payment-methods/2018/consumer-trends-mobile-voice-biometrics-cash/

Experian. (2019, January). 2019 Global Identity and Fraud Report. Retrieved from https://www.experian.com/blogs/news/2019/01/30/global-identity-and-fraud-report/

Experian. (2020, January). 2020 Global Identity and Fraud Report. Retrieved from https://www.experian.com/decision-analytics/global-fraud-report

NuData Security (undated). Online Account Origination Fraud: When New Users Are Bad News [blog post]. Retrieved from https://nudatasecurity.com/resources/blog/online-account-origination-fraud-when-new-users-are-bad-news/

NuData Security. (2019, February 7). Fraud Fighting Technologies Protected Consumers and Saved Retailers Millions This Holiday Season [blog post]. Retrieved from https://nudatasecurity.com/press/fraud-fighting-technologies-saved-retailers-millions-this-holiday-season/

GIACT/PYMNTS. (2019, December). The Fraud That 85 Percent Of Fraud Detection Systems Miss. [blog post]. Retrieved from https://www.pymnts.com/news/security-and-risk/2019/synthetic-fraud-evolution-prevention-tools/

Stone, J. (2019, June 17). When Your Apps are Dormant, You Become a More Likely Target for Crooks [blog post]. cyberscoop. Retrieved from https://www.cyberscoop.com/account-takeover-attacks-ato-datavisor-research/

Experian/AITE Group. (2020, May 5). Experian Releases New Version of Its Integrated Digital Identity and Fraud Risk Platform to Help Businesses Quickly Respond to Today's Emerging Fraud Threats [press release]. Retrieved from https://www.businesswire.com/news/home/20200505005271/en/Experian-Releases-New-Version-Integrated-Digital-Identity

Weiss, E. (2019, April 11). Kaspersky Lab Unearths Dark Web e-Shop that Sells Stolen Digital Identities [blog post]. Retrieved from https://findbiometrics.com/kaspersky-lab-unearths-dark-web-e-shop-sells-stolen-digital-identities/

Kaspersky Lab. Kaspersky Lab Uncovers Genesis: The Underground E-Shop with Tens of Thousands of Digital Doppelgangers for Sale to Bypass Financial Anti-Fraud Solutions [press release] Retrieved from https://www.businesswire.com/news/home/20190409005574/en/Kaspersky-Lab-Uncovers-Genesis-Underground-E-Shop-Tens.

Hodge, R. (2019, December 27). Welcome to the 2019 Data Breach Hall of Shame. Retrieved May 07, 2020, from https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/