Retail fraud: Key trends and prevention strategies

Understand the emerging threats, and how retailers can protect themselves and their customers.

eBook
Nuance Gatekeeper

Retail fraud is an agile business.

Criminals constantly find new ways to attack brands and their customers, rapidly switching tactics, channels, and targets. But retailers don't have to get stuck playing catch-up.

By understanding both their own vulnerabilities and global trends in retail fraud, brands of every shape and size can take practical steps to minimize fraud losses without adding friction to shopping and service journeys.

In this guide, we explore current and pressing trends in retail fraud. We also outline strategies for combating the most prevalent types of attack—from fraudulent CNP purchases in digital channels to extended warranty fraud and abusive returns.

1 Opus Research
2 https://www.experian.com/content/dam/noindex/na/gda/Experian_Global_Identity_and_Fraud_Report_2021.pdf
3 https://risk.lexisnexis.com/insights-resources/research/2020-true-cost-of-fraud-retail
4 https://risk.lexisnexis.com/insights-resources/research/2020-true-cost-of-fraud-retail

Retailers are strengthening fraud prevention

For better shopping experiences—

55%

of consumers say security is their top priority for their online experience[1]

85%

don't like current authentication processes[2]

For reduced losses and costs—

$3.36

for every $1 lost—The cost of fraud to retailers[3]

7.3%

How much this cost has risen over the last year[4]

Retail fraud: The key trends

Last year, US mid/large retailers saw a 43-48% increase in successful fraud attacks.[5]

1. New shopping journeys have created new vulnerabilities

Like water seeping into a basement, fraud always finds the path of least resistance.

As retailers have adapted to the extraordinary challenges of 2020 and 2021, criminals have adapted too, finding and exploiting weak points in security measures. The most critical vulnerabilities for any given retailer will depend largely on its size and digital maturity.

Vulnerabilities for smaller retailers

Many mom-and-pop stores and small retailers started 2020 without an e-commerce site. To meet customers where they were in the midst of the pandemic, they rapidly created digital storefronts, but without fully understanding the risks involved.

Suddenly they found themselves:

- Shipping items before banks have time to flag a transaction as suspicious
- Failing to look for common fraud indicators like suspicious shipping addresses
- Failing to properly confirm the identity of people collecting BOPIS[6] orders

Vulnerabilities for larger retailers

Most large, well-established retailers have mature digital storefronts and understand the telltale signs of fraud. As they've secured their online business, however, they haven't made similar investments in their contact center and IVR.

As a result, fraudsters are now targeting larger retailers through their comparatively under-protected phone channels, looking for a human agent they can manipulate.

Many of those agents have been working from home, isolated from their supervisors and colleagues. They've also faced new and greater stresses and financial pressures.

This makes agents more vulnerable to fraudsters' attempts at social engineering. But it also means that they—and the people they live with—have more opportunities and greater motivation to commit fraud themselves, for example, by stealing and selling the personal details of the customers they serve.

5 https://risk.lexisnexis.com/insights-resources/research/2020-true-cost-of-fraud-retail
6 Buy online, pick-up in store.

2. Malware-assisted takeovers are on the rise

Malware that lets fraudsters take over shoppers' accounts and devices is already rife in parts of Europe—and on its way to North America. The story of the rise of the TeaBot and FluBot malwares highlights the insecurity of two-factor authentication via push notification-based one-time passcodes.

Retailers must now familiarize themselves with these threats and take steps to reduce the risk of authorizing fraudulent transactions on their digital channels.

The threat from TeaBot

A new and increasingly popular malware is hidden in fake versions of Android mobile apps. Once a user downloads the fake app, "TeaBot" can log their keystrokes, perform overlay attacks, intercept text messages and Google Authentication codes, and even take complete, remote control of the infected device.[7] This offers criminals multiple avenues to steal a user's passwords and payment information and make fraudulent purchases.

At present, TeaBot is most prevalent in Spain, Italy, and the Netherlands, but researchers expect it to spread quickly.[8]

The threat from FluBot

FluBot also targets Android users but is most commonly distributed through SMS-based phishing attacks.

In a FluBot attack, the victim receives a fake package delivery notification with a link to a fake package tracking app—which actually contains the malware.

Once downloaded, FluBot requests access to the user's contacts so it can replicate the attack on the devices of their friends, family, and colleagues. Then it requests the permissions it needs to perform overlay attacks on banking apps and circumnavigate one-time passcodes and two-factor authentication checks.[9]

Most FluBot attacks are currently taking place in mainland Europe, but the malware is also gaining traction in the UK and should be on the threat radar of retail brands everywhere—especially retail banks.

The global cycle of fraud threats

Fraud schemes typically start—and are refined—in one area, but then quickly travel around the world. For example, when chip cards were introduced in Europe, fraudsters switched their focus to Canada's retailers. When Canada's adoption of chip cards reached critical mass, they switched to the US.

7 https://www.cleafy.com/documents/teabot
8 https://labs.bitdefender.com/2021/06/threat-actors-use-mockups-of-popular-apps-to-spread-teabot-and-flubot-malware-on-android/
9 https://www.nortonlifelock.com/blogs/norton-labs/flubot-targets-android-phone-users

For retailers, fraud prevention has always been a balancing act.

3. New legislation and protocols are bringing new challenges and opportunities

The need to keep the barrier high against fraudsters must be weighed against the desire to make shopping, shipping, and refunds as quick and painless as possible for legitimate customers. Retailers that fail to deliver fast, frictionless experiences risk not living up to the expectations set by the industry's largest players, thereby losing market share.

So, as new legislation and protocols are introduced to protect consumers, the smartest retailers are planning ahead to ensure that stronger security comes with a smoother shopping experience.

The risk of tighter security damaging sales

Retailers have reason to tread lightly. In Europe, merchants have seen conversion rates fall following the introduction of Strong Customer Authentication (SCA) in December 2020 as part of the EU's broader PSD2 legislation. The UK's Financial Conduct Authority has pushed its own deadline for compliance with SCA until March 14, 2022, "to ensure minimal disruption to merchants and consumers".[10]

The opportunities—if retailers get it right

The 3D Secure security protocol—which underpins services including Verified by Visa and American Express SafeKey—has now evolved into 3D Secure 2.0, which supports compliance with SCA and provides greater protection against chargebacks.

The new protocol offers retailers the chance to use stronger, biometrics-based authentication when challenging suspected fraudsters and reduce shopping friction in the process.[11]

10 https://www.finextra.com/newsarticle/38102/fca-extends-sca-deadline-by-a-further-six-months
11 https://midigator.com/blog/3d-secure-2-0/

4. New technology is eliminating the high costs of knowledge-based authentication

Biometrics technology is also set to help retailers tackle the multiple costs and lost sales associated with traditional, knowledge-based authentication (KBA).

By allowing brands to authenticate customers seamlessly and securely based on who they are—rather than a password or PIN they know, or a device or token they have—biometrics can reduce not only fraud-related costs, but also lower operational costs and cart abandonment rates.

The cost of KBA: Fraud-related costs

According to a study by American Express, 69% of merchants in the US are spending significant company time and expenses dealing with payment fraud.[12]

This is partly because KBA is no longer a robust deterrent to fraudsters, who can simply buy or hack their way into a shopper's account:

— 15 billion account username-password combinations are for sale online, including bank accounts[13]

— A study of more than 1 billion leaked credentials found 42% to be vulnerable to quick dictionary attacks and 1 in 142 to be "123456"[14]

— ~70% of the world's most popular passwords can be cracked in less than a second[15]

The cost of KBA: Lost sales

Other research suggests that passwords and passcodes reduce retailer revenue by acting as a barrier for would-be shoppers:

— 1/3 of online purchases are abandoned at checkout because consumers cannot remember their passwords – Mastercard and Oxford University[16]

— 68% of US shoppers have abandoned an online purchase due to forgetting a password, trouble logging in, or issues receiving a one-time passcode – Visa[17]

— 8 in 10 US merchants agree their online checkout experience needs to be simplified for their customers – American Express[18]

What's more, a lost sale can often be the prelude to a lost customer. According to Gartner, 96% become more disloyal after high-effort service interactions.[19]

12 https://network.americanexpress.com/globalnetwork/dam/jcr:09c34553-b4a2-43ca-bf3e-47cbc911ea51/American Express 2019 Digital Payments Survey_Insights Paper.pdf
13 Digital Shadows study reported via ZDNet, July 2020
14 https://www.zdnet.com/article/one-out-of-every-142-passwords-is-123456/
15 https://www.techrepublic.com/article/most-of-the-worlds-most-popular-passwords-can-be-cracked-in-under-a-second/
16 http://www.cs.ox.ac.uk/files/9113/Mobile Biometrics in Financial Services.pdf
17 https://usa.visa.com/visa-everywhere/blog/bdp/2020/01/02/banking-on-biometrics-1578003687083.html
18 https://network.americanexpress.com/globalnetwork/dam/jcr:09c34553-b4a2-43ca-bf3e-47cbc911ea51/American%20Express%202019%20Digital%20Payments%20Survey_Insights%20Paper.pdf
19 https://www.idrnd.ai/wp-content/uploads/2020/04/IDRD-BIOMETRICS-TO-THE-RESCUE.pdf

$5M to $20M

the cost per year for large organizations to handle password-reset inquiries[20]

53
SECONDS

AHT saved on average using voice biometrics for faster authentication[23]

The cost of KBA: Password resets

Handling password-reset inquiries can account for up to 6% of contact center activity, costing larger organizations between $5 million and $20 million a year.[20]

It's not just customers who forget their passwords; employees do, too. This can add another huge expense for organizations and their IT teams. Forrester reports that large organizations spend up to $1 million each year in staffing and infrastructure expenses just to handle password resets, and that a single reset costs, on average, $70 in labor.[21]

The cost of KBA: Average handle time

Knowledge-based authentication is slow. Whatever the channel, your brand has to ask for something and your customer has to respond—adding as much as 20% to a contact center's average handle time (AHT).[22]

Companies that switch to voice biometrics authentication in their phone channels, on the other hand, see AHT fall by an average of 53 seconds through faster authentication[23]—reducing operational costs, and improving productivity for agents who can handle more calls even while delivering better, more personal service.

20 https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/is-cybersecurity-incompatible-with-digital-convenience
21 https://www.helpnetsecurity.com/2019/04/12/password-less-security-benefits-helpdesks/
22 https://www.home.neustar/blog/how-covid-19-reshaped-inbound-authentication
23 Average reduction in AHT is calculated based on the results seen by 10+ Nuance customers following the implementation of a voice biometrics solution

Practical fraud prevention for retailers

Brands can and should take practical steps to address many of the threats discussed in this ebook.

Stop fraudulent purchases on phone channels

A typical scam

— A fraudster targets a retailer through its contact center.

— They talk to the agent and buy the latest smartphone using stolen credit card details.

— They opt for BOPIS, so they don't have to provide a shipping address or intercept a delivery.

— They send a runner to do the pick-up to minimize their risk of getting caught.

The solution: Spot fraudsters before they reach an agent

— The retailer should screen the incoming call with an AI-based risk engine, factoring in evidence of number spoofing and repeat withheld calls.

— The fraudster's first contact should be with a conversational IVR that uses biometrics to match their voice against a watchlist of known fraudsters, and clustering technology to detect if the same voice is repeatedly calling in.

— When the call is flagged as suspicious it should be directed straight to the retailer's fraud team.

— If the fraudster does manage to reach an agent, conversational biometrics technology should analyze their words, themes, and pacing to detect a suspicious interaction and raise the alarm.

The benefits

— The retailer prevents fraud before it happens, reducing losses and costs.

— It protects agents against social engineering—improving agent experience, and helping to reduce absenteeism and employee turnover.

— It saves on the cost of training agents in authentication procedures, and—because biometrics can deliver higher accuracy than traditional, transaction-based fraud systems—it sees a reduction in manual fraud review workloads.

Stop fraudulent purchases on digital channels

A typical scam

— A fraudster uses the malware on a customer's device to steal their sign-in details for their favorite retail brand.

— The fraudster logs in and buys multiple pairs of designer sneakers using the saved credit card, dispatching to the address of a local Airbnb.

— They use their control of the customer's device to circumvent any additional security checks and wait to intercept the delivery.

The solution: Continuously authenticate customers online

— The retailer should use behavioral biometrics to constantly authenticate its customers while they're logged in, based on how they usually type, swipe, and hold their device.

— When the retailer spots unusual behavior and challenges the user to sign in again, it should ask them to use an inherent authentication factor—like the sound of their voice—that the malware can't steal.

The benefits

— The retailer prevents fraud before it happens, reducing losses and costs without adding friction to the shopping journey of legitimate customers.

— When a customer is asked to reauthenticate themselves, they're spared the hassle of having to remember a password or generate and enter codes.

— The use of a stronger "inherence" factor—in this case, voice—in the retailer's two-factor authentication process also helps to prevent family fraud; even someone with access to a customer's mobile device and password won't be able to replicate their voice.

Stop extended warranty fraud

A typical scam

— A customer buys a top-of-the-range gaming PC and takes out an extended warranty. Some months later, a fraudster acquires the authentication credentials for their account.

— The fraudster calls the retailer's contact center posing as the customer. They claim the PC's GPU has failed and ask for a replacement.

— The retailer must spend time and money investigating the claim (and potentially infuriate a customer experiencing a legitimate fault) or honor the terms of the warranty and ship the expensive replacement part—straight into the hands of the fraudster.

The solution: Authenticate customers using inherent factors

— The retailer should enroll the customer into a strong biometric authentication program when they purchase the extended warranty—for example, by asking them to register their voiceprint.

— When the fraudster calls to make the claim, their voice should be compared against the customer's voiceprint, so the call can be immediately flagged for the attention of the retailer's fraud team.

The benefits

— The retailer prevents the loss of its goods and saves the time and resources it might have spent validating the claim.

— It also builds up valuable data to further improve their fraud detection systems, including information on the caller's device, phone number, and script used.

Using AI to monitor agent compliance

Retailers can also use technology to help their agents stay on the right side of the law when selling extended warranties. As well as monitoring conversations for signs for fraud, AI can listen to make sure that agents ask for customers' explicit consent before they add the warranty to their order—helping to avoid bad surprises when the bill arrives.

Stop abusive returns

A typical scam

— A fraudster purchases an expensive guitar online. As soon as it arrives, they call up to say that it's scratched, and they want to return it.

— The fraudster sends back a box full of rocks, and the retailer processes the refund before the fraud is spotted.

— The fraudster now has their money back and a new guitar to sell, while the retailer has lost both the item and its purchase price.

The solution: Boost proactive fraud prevention capabilities

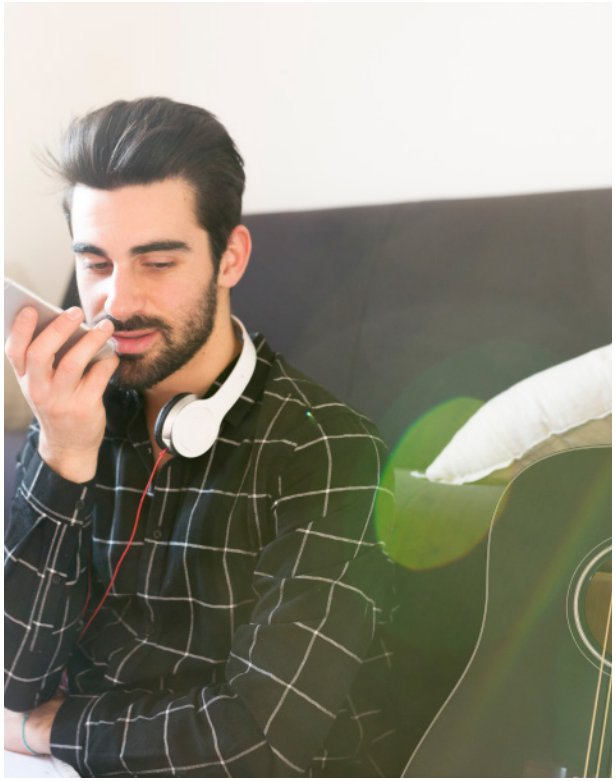
— The retailer should implement a robust AI risk engine that uses voice biometrics and other factors to proactively identify fraudsters when they call (see "Stop fraudulent purchases on phone channels").

— The risk engine can also include conversational biometrics to detect social engineering or fraud mules hired to follow a script.

The benefits

— The retailer reduces its fraud losses and deters less-experienced fraudsters from making future attempts.

— At the same time, it gathers even more data about repeat offenders, including associated devices, phone numbers, and scripts.



It’s time to futureproof your fraud prevention

In the last year, we’ve seen the level of investment in fraud prevention and authentication skyrocket. Thanks to cloud delivery models, we’ve also seen key technologies like biometrics come within the reach of retailers of every size.

Wherever your immediate fraud prevention challenges lie, now is the time to consider how you can make strategic use of technology to step up security and reduce friction for legitimate customers, across every channel.

If you’d like our advice, don’t hesitate to get in touch.

Our Chief Fraud Prevention Officer, Simon Marchand, has more than a decade of experience in fraud prevention. As well as sharing his own expertise, he can introduce you to organizations facing similar challenges and exploring similar technologies; more than 1,500 leading brands, including five of the nine largest global retailers, already trust Nuance solutions.

Next steps

— Get in touch with our experts:
Email cxexperts@nuance.com

— Learn more about Nuance solutions:
Visit www.nuance.com/fraud

Simon Marchand, CFE,
Adm.A. Chief Fraud Prevention Officer,
Nuance Communications

Simon has been working in fraud prevention for over ten years. Before joining Nuance, he held key fraud management positions at Bell Canada and Montreal-based Laurentian Bank, and was a professional inspector at Québec’s order of chartered administrators.

About Nuance Communications, Inc.
Nuance Communications (Nuance) is a technology pioneer with market leadership in conversational AI and ambient intelligence. A full-service partner trusted by 77 percent of U.S. hospitals and 85 percent of the Fortune 100 companies worldwide, Nuance creates intuitive solutions that amplify people’s ability to help others.

ENT_4426_01_EB, Aug 24, 2021