Fraud.net

Protect Your Customers and Company this Holiday Season

Build a More Secure Digital Customer Journey

Gartner

Fraud.net was recently recognized in the 2021 Gartner Market Guide for Online Fraud Detection.

Table of Contents

Is Your Organization Prepared for the Holidays? // 1

Creating Digital Trust for Your Customers // 2

Securing the Digital Customer Journey // 3

Digital Customer Journey Scenarios // 5

Next Steps // 11

Is your organization prepared for the holidays?

An Accenture study found that there was a triple-digit year-over-year increase in cyberattacks during the first half of 2021.

Unfortunately, this year's holiday season is shaping up to possibly be a record-setter for fraud. Let Fraud.net help improve your customer's experience while protecting your organization and customers from fraud throughout their digital journey.

IT'S THE HOLIDAY FRAUD SEASON

COVID's impact is slowly diminishing, but fraudsters are not letting up on their attacks. Seemingly daily, we are seeing highly visible attacks against organizations big and small, from the government to digital merchants. With pent-up demand likely adding to the already increased fraud volumes of the holiday - the 2021 holiday season, without more focus on preventing fraud, is likely to be a most wonderful time for cybercriminals.

Criminal's schemes are increasing in sophistication, as the opportunities presented by the pandemic helped them ramp up their capabilities.

The holidays are the opportune time for cybercriminals to deploy their schemes:

- Continued high levels of online sales due to lingering COVID concerns impacting in-store purchases.
- First-party chargeback (friendly) fraud is increasing as fraudsters take advantage of lax anti-fraud measures during the post-purchase stage of the journey.
- Digital retailers have to contend with credit card fraud, plus fraud via gift cards, buy-now-pay-later (BNPL), and various mobile payment applications.
- The holiday season's increase in volume provides fraudsters with better cover to ply their trade.

Creating Digital Trust for Your Customers

The digital customer experience has been defined as "the sum total of any online interaction that a consumer has with your brand." For your business to reach a best-in-class customer experience, you also need best-in-class cybersecurity to provide the digital trust that your customers require.

A Best-in-Class Digital Journey

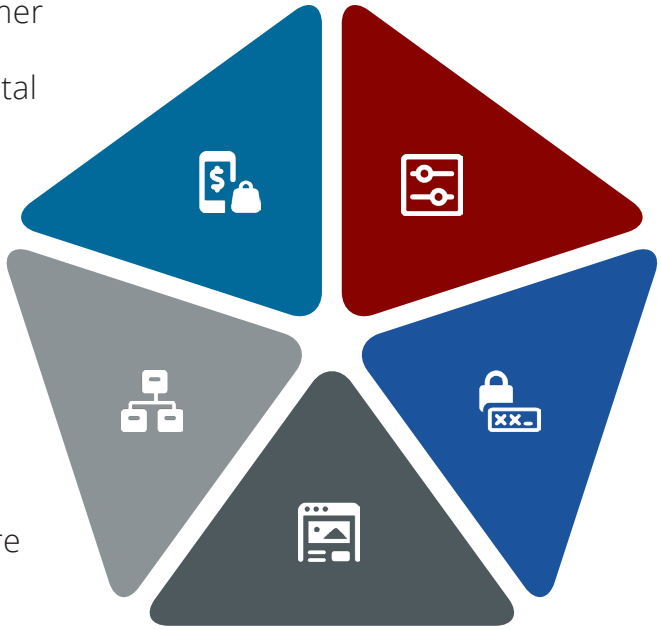
According to McKinsey, below are the five items necessary to develop a best-in-class secure digital customer journey:

1 Understand Your Customer

Develop consumer "personas" and appropriate digital journeys.

2 Develop Controls

Apply consumer identity-access-management controls for prioritized journeys.



3 Focus on Security and Experience

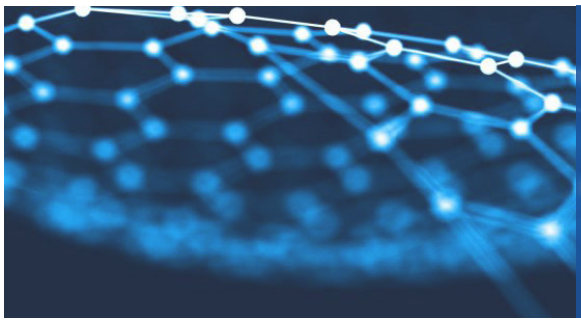
Create a reasonable balance between security and the customer experience.

4 Build Flexible Architecture

Design for both flexibility and enabling new business value.

5 Create Systems

Build strong governance mechanisms to support a secure journey.



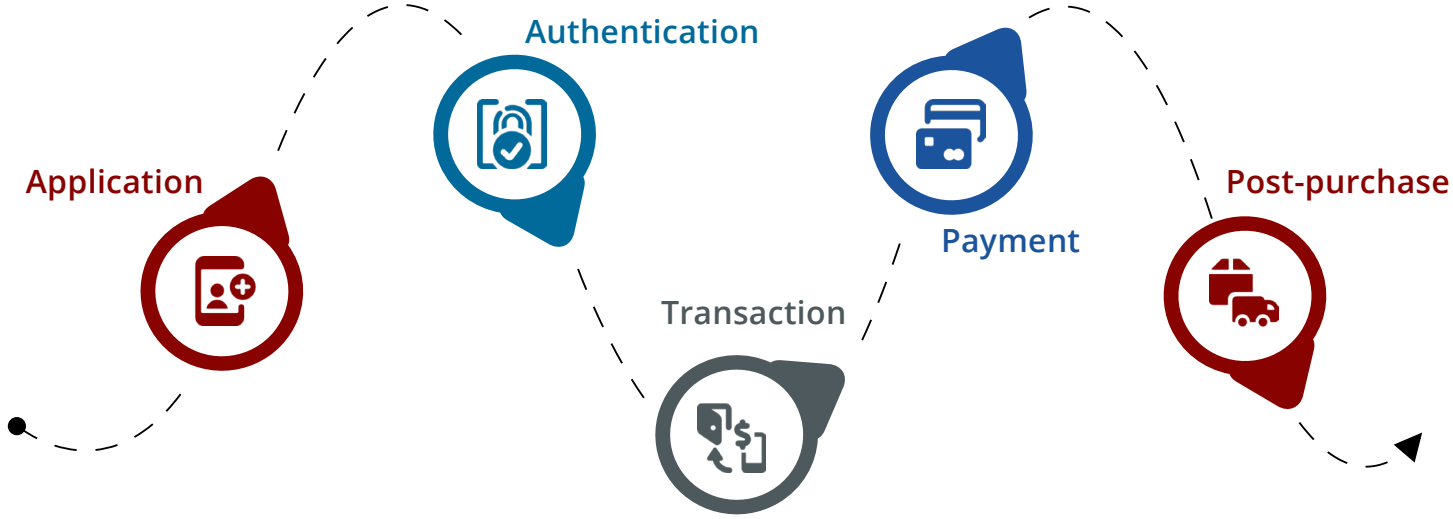
In PwC's survey of business and technology executives regarding Digital Trust, almost 50% of Retail and Consumer leaders stated, "...they now bake cybersecurity and privacy implications into every business decision and into their planning."

PwC Global Digital Trust Insights

Securing the Digital Customer Journey

Fraud can occur throughout the digital customer journey.

Organizations are rapidly coming to the realization that digital security and trust are critical parts of the customer experience. Therefore, companies need to ensure advanced fraud prevention measures are in place throughout the digital customer journey:



A heavy-handed approach brings its own risks...

However, securing your customer's experience is more than just "locking down" your systems to make it difficult for fraudsters. Doing so will result in a **rapid increase in false positives**, and **create severe issues** for your customers and business.

Increased customer friction and, often, abandonment of your site.

Reputational damage to your company through negative reviews and word-of-mouth.

Additional financial costs because of the excessive time required by your fraud team in case management.

"Just like the animal kingdom, any sign of weakness breeds vulnerability, so being aware of industry and geographic impact patterns, coupled with sound threat intelligence, can help to counteract determined threats."

2021 Accenture study - "Triple digit increase in cyberattacks: What next?"

Solutions to Create a Safer Journey

Fraud.net's comprehensive AI-based platform is a leader in the industry and offers unmatched modularity and flexibility. Companies work with Fraud.net to:

- Decrease fraud and risk
- Lower the queue workload
- Automate manual processes
- Reduce false positives
- Improve approval rates
- Increase revenue and profitability

Using Fraud.net's comprehensive platform and products, your company can prevent a variety of fraud with our tools:

Application AI
Provides a real-time risk assessment of applications to verify legitimate customers while halting fraudsters.

Login AI
Stops account takeovers from ruining your business and customer's holiday by screening and verifying key details of user's sign-in.

Transaction AI
Helps deliver a frictionless customer experience, while reducing payment fraud, BNPL abuse, friendly fraud, and other schemes.

Digital Customer Journey Scenarios

Below we present critical steps in a typical digital customer journey with online merchants, illustrated through multiple scenarios and personas. We've included **three personas** with both good and "evil" customer profiles within **six scenarios** that can occur during the holidays. The scenarios describe the potential actions of the personas and how Fraud.net protects organizations and their customers from fraud.

Olivia
- Holiday Shopper
- Business owner
- High-end gift buyer

Nick
- Organized crime member
- "Friendly Fraud" perpetrator

Emily
- Leads small criminal enterprise
- Uses buy now, pay later scheme to steal

1A OLIVIA'S HOLIDAY PURCHASE FOR HER EMPLOYEES

The Scenario: Olivia owns an engineering company and every year purchases holiday gifts for her employees. She is a long-time customer of Marley's Sundries, where she buys her employees gifts.

Unbeknownst to her, the account with Marley's is being attacked by fraudsters in an account takeover. A lone fraudster, knowing that the holidays' higher volumes and distractions make fraud simpler to deploy, purchased stolen credentials, including Olivia's, on the dark web.

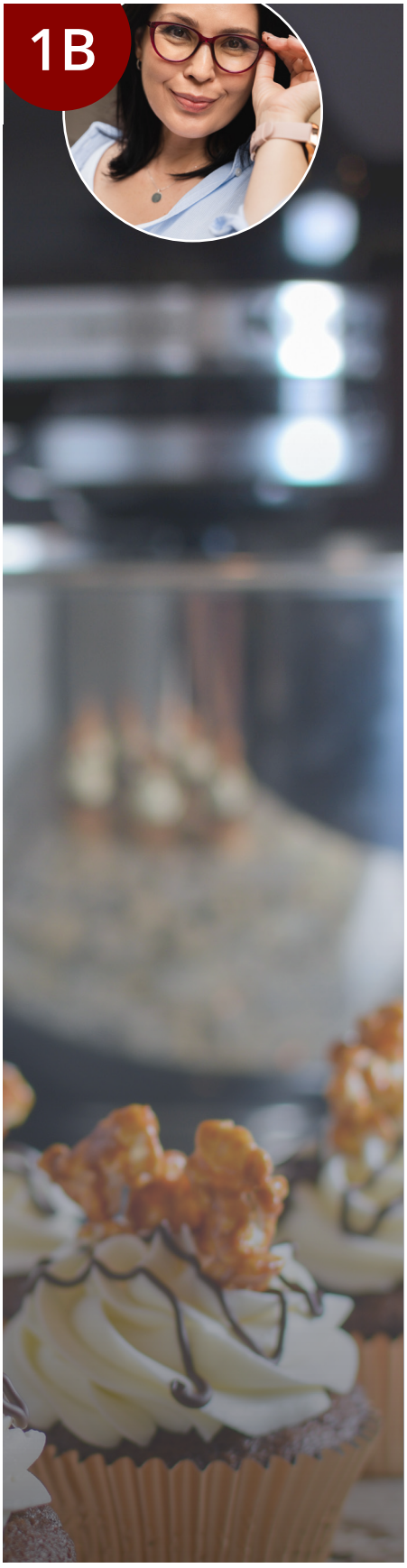
Marley's legacy anti-fraud system is outdated and an amalgamation of one-off tools, combined with systems from mergers and acquisitions.

Outcome: Unfortunately for Olivia, the criminal, using credential stuffing, changed the shipping address and password, and purchased a substantial amount of items from Marley's on her account.

The Fraud.net Solution: If Marley's was a client of Fraud.net, Olivia's account would have been protected against this fraud.

At login, **Fraud.net's Login AI** would have checked if a different IP address and device were used in the transaction compared to her previous transactions.

Login AI helps protect organizations against account takeovers and other unauthorized activities by screening and verifying essential details about devices used when signing into an account. As a result, it can put a halt to cybercriminal's credential stuffing, and other methods in trying to gain access to customer's accounts.



OLIVIA'S HOLIDAY PURCHASE FOR HER MOTHER

The Scenario: Olivia also wants to buy her mother a holiday present, a new kitchen stand mixer, so she begins exploring her buying options. After investigating various options, she decides on a model available from the retailer Valdivian's online store.

1. She starts by creating an account with Valdivian, which is a client of Fraud.net.
2. The Application AI product ingests the data from Valdivian, and using Fraud.net's proprietary datasets and the many third-party APIs available via our AppStore, enriches the application data.
3. The account information she provides is checked against Fraud.net's Collective Intelligence Network to analyze if her associated data elements have ever been involved in fraud activity.
4. The enriched application data is then assessed by Fraud.net's rules engine and viewable in the case management portal. Both rules-based and machine learning scores are assigned to each transaction.

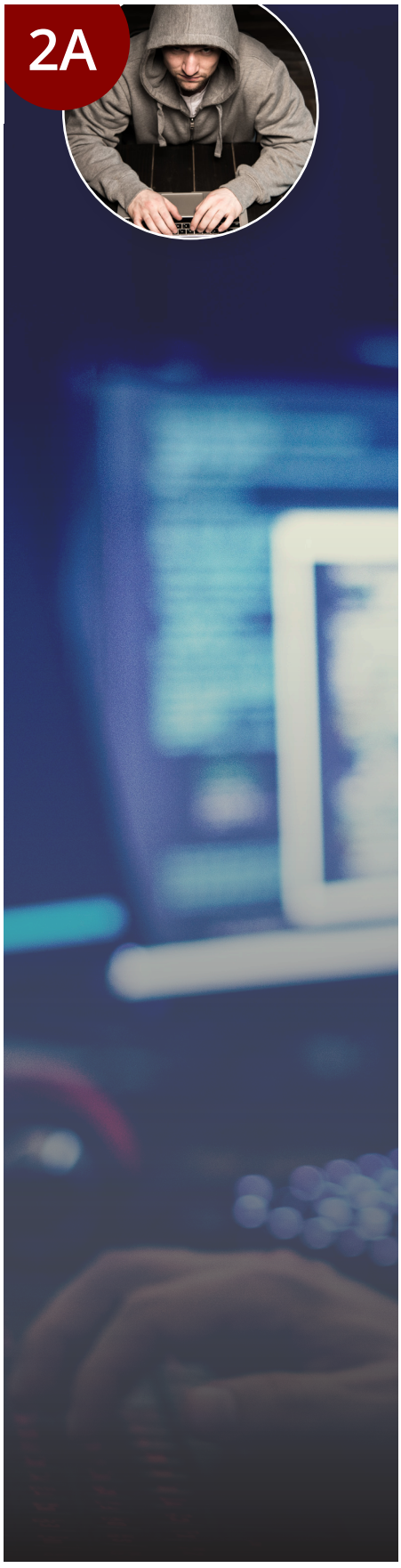
The Fraud.net Experience: Based on this wealth of data, within seconds, Valdivian approves Olivia's application.

At checkout, she uses her personal credit card to purchase the item for her mother.

Fraud.net's Transaction AI product provides comprehensive risk assessment in fulfilling the transaction.

This assessment includes verifying if the card has been used in any transactions with fraudulent outcomes, activities indicative of her details being available on the dark web, or recent changes to the billing address or other data elements.

As a result of Fraud.net's products, Valdivian has a highly secure, frictionless process for Olivia and their other customers.



NICK THE FRAUDSTER'S FRIENDLY FRAUD SCAM

The Scenario: Nick is part of an organized criminal gang that employs many fraud schemes, but for the holidays is focusing on friendly chargeback fraud. They plan to take advantage of companies' disparate systems, siloed data, and the volume and distractions of the holidays.

The group has targeted a new upscale jewelry store, Moly. The company is already known for its customer service and liberal return policy. By timing their fraud during the rush of the holidays, along with the new store's many new employees, creates more opportunities for Nick's gang.

The Fraud Scheme : Moly's systems do not include robust anti-fraud measures.

Since Moly's is not a Fraud.net client, they do not detect the typical anomalies and patterns in the sequence of actions involving friendly fraud.

The fraudsters are able to deploy a variety of first-party fraud schemes, including:

1. Calling the issuing bank to falsely claim that a delivered item was not received.
2. Returning fake items instead of the actual merchandise.
3. Falsely informing the card issuer, they returned a product and never received the refund.
4. Telling the issuer that a product ordered online is defective.

The Aftermath: The systems and tools that Moly currently has available leaves gaps and creates data silos in their coverage of returns and refunds. In addition, its Fraud team is already far behind in reviewing their manual review queues. All of these factors, when combined, create opportunities for criminals like Nick and his cohorts.

-25% Moly does not realize it yet, but friendly fraud is taking a 25% bite out of their profits. A substantial profit drain and problematic for any retailer to sustain long-term.

NICK THE FRAUDSTER'S FAILED FRIENDLY FRAUD

The Scenario: Nick's team of criminals is also targeting another retailer to deploy friendly fraud - Jovie Jewelers.

With the high-priced items sold by the retailer, the fraudsters believe they have an easy target for pulling off their chargeback fraud.

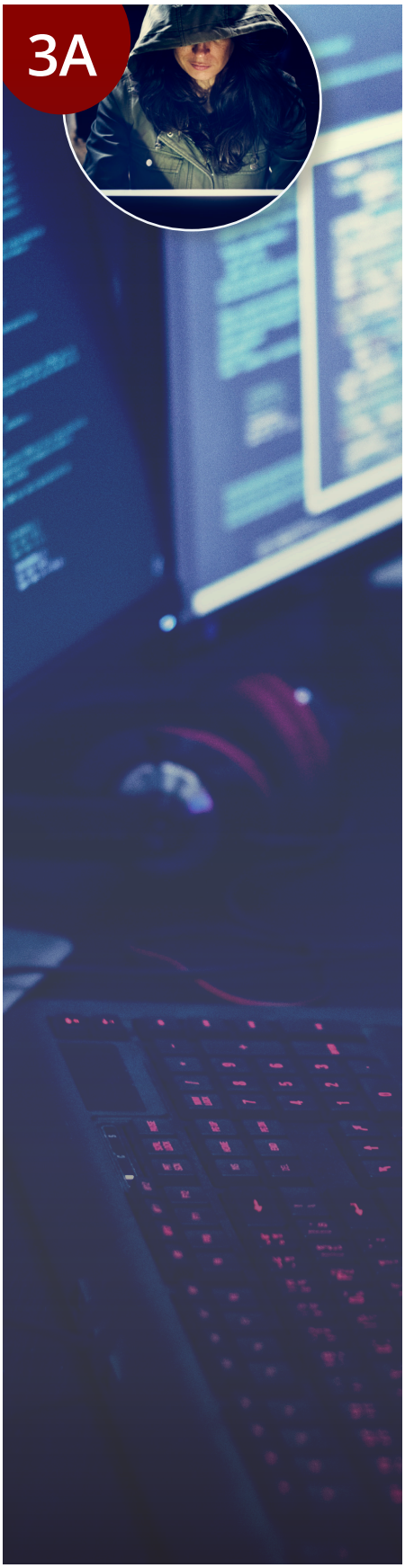
They plan to utilize the same friendly fraud schemes described earlier.

But Jovie's is a Fraud.net client and utilizes their AI-based platform of tools, including Login AI, to help detect and prevent fraud.

1. With Login AI, Jovie's Fraud team can quickly detect anomalies and patterns in the sequence of actions involving the account.
2. Jovie's Fraud team immediately noticed a device previously associated with fraud was trying to buy jewelry.
3. Another Fraud.net product, Transaction AI, has powerful AI models to help businesses like Jovie's, detect fraud before it can occur. The product also provides their Fraud team with real-time, actionable alerts and fully explainable risk scores for every transaction.
4. Transaction AI also helps them quickly visualize fraud trends through the powerful analytics available in the Fraud.net platform.

The Fraud.net Experience: Using Transaction AI, the fraud team can detect the chargeback fraud schemes used by Nick's gang and shut them down before more damage occurs.

The strength of Fraud.net's algorithms helps Jovie's reduce false positives, improve the effectiveness of their fraud team, and enhance their customer's experience.



EMILY'S TEAM OF BNPL FRAUDSTERS

The Scenario: Emily has been leading a small team of criminals engaging in a variety of fraud schemes. One of their favorite schemes is to target retailers that offer "buy now, pay later" (BNPL) as a payment option.

The Fraud Scheme: Her specific target is high-end TVs, since the demand rises during the holiday season, and she has international contacts to resell the stolen items.

Her plot purchases TV's in lots of 3 - 6, using stolen identities to sign-up for BNPL, and then has the TVs shipped to a warehouse in Florida for reselling and shipping on to South America.

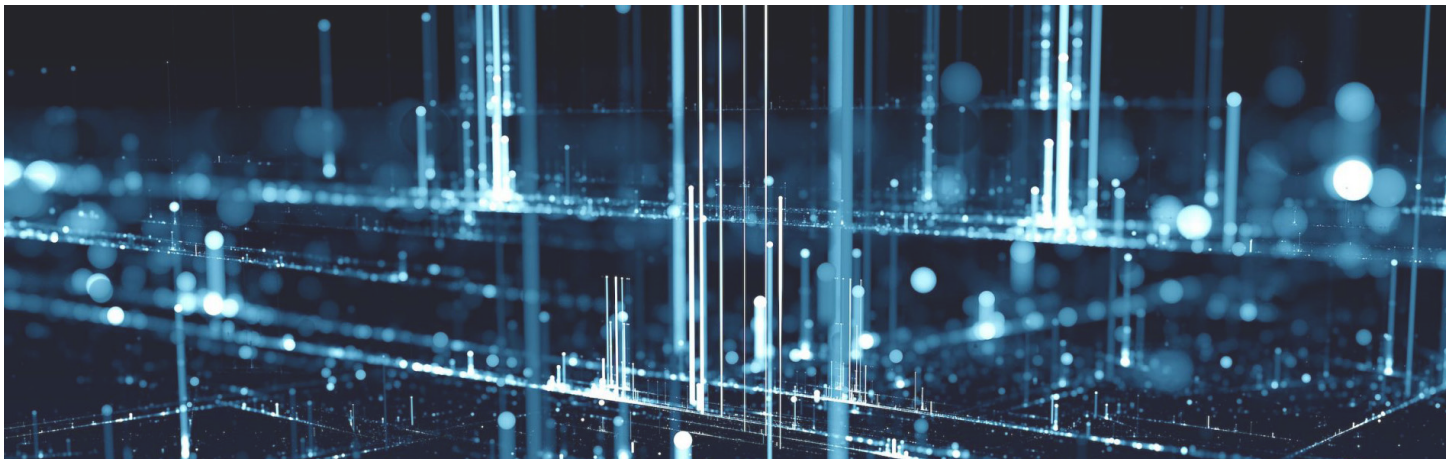
The Target: They hone in on XLTV Emporium, which offers BNPL as a payment option for most of their merchandise. XLTV is not a client of Fraud.net and uses legacy systems that were modified in-house to accommodate BNPL, including their anti-fraud system.

But their legacy system does not provide any history information on previous BNPL transactions.

A wealth of data is vital in identifying potential BNPL fraud. With an understanding of the links from IP addresses to fraudulent purchases from other commerce sites, a company can be tipped off to likely BNPL fraud.

The Impact: Unfortunately for XLTV, Emily's small team was able to purchase six TVs with BNPL terms, using stolen identities bought on the dark web.

They modified shipping addresses to a warehouse in Florida for reselling and shipping to South America. For XLTV, they were victims of first payment default for the six high-priced TVs.



3B EMILY'S BNPL FRAUD FOILED

The Scenario: Emily's gang of cybercriminal's next target is Silver & Gold Electronics and their new BNPL plans. One of her cohorts purchased five TVs via a BNPL plan with a stolen identity. Fortunately, Silver & Gold Electronics is a client of Fraud.net and utilizes the Application AI and Transaction AI products to protect their BNPL plans from fraud.

The Defence: Before their customers can finalize the transaction, they must apply for credit through a short online form using Application AI. In the Application AI tool, among other checks, is an analysis of billing addresses for previous bad outcomes, and the velocity of the shipping address' usage. Providing a world-class customer experience is essential to Silver & Gold; the BNPL option was important for them to meet the growing demand by their customers, especially in the younger demographics. In addition, they were aiming to reduce cart abandonment and boost average order value.

The Fraud.net Experience: Fraud.net's platform helps Silver & Gold review their applications for any associations with fraud. These comprehensive and rapid checks stop further fraud. For approved applications at the point of transaction, Fraud.net evaluates with a number of analyses, including velocity and linkages, to ensure the transaction is associated with the right person.

Especially for high-risk items, like TVs, analysis of the number of times purchased by an IP address, or multiple shipments to other locations by an IP address, provides an excellent indicator of fraud.The Transaction AI tool helps ensure there are no data elements related to previous fraud transactions. Many times shipping will be to a drop address and results in a high volume of activity for a shipping address along with multiple bill-to addresses.

Fraud.net provides a detailed history of previous BNPL transactions, which is crucial in identifying potential BNPL fraud. Understanding the links from IP addresses used in purchases at other merchants where fraud has occurred, offers vital insights into potential BNPL fraud.

As a result of Fraud.net's tools, Silver & Gold Electronics was able to prevent Emily and her group from perpetrating BNPL fraud.

Ready to learn how Fraud.net can protect your bottom line and your customer experience this holiday season?

You need a helping hand during the holidays. Let Fraud.net's flexible AI-powered platform help your organization detect and prevent fraud. Our powerful tools help online retailers stay ahead of fraudsters by closely tracking and trending suspicious activity with easy-to-use tools.

At Fraud.net, our mission is to make every digital transaction safe and your business more profitable. Contact our experts today to discuss your organization's needs and a demonstration of how we can help your organization prevent fraud and thrive during the holiday fervor.

Access Fresh Insights from Every Fraud.net Product:

Our full suite of products can be tailored to provide the fraud protection system best suited to your needs

Email AI™ | Login AI™ | Transaction AI™ | Application™ | Account AI™ | Device AI™

LEARN MORE

 | sales@fraud.net | 866.971.2030