UNLOCKING MERCHANT INNOVATION USING MACHINE LEARNING FOR FRAUD
INTRODUCTION

The world of eCommerce lost $60 billion in fraud in 2017.¹ And beneath this massive figure there’s a world of additional pains.

Fraud results in:

» Losing money to chargebacks and spending time disputing them.
» Declining legitimate customers due to poor fraud controls.
» Losing stolen goods and the money spent on shipping.
» Bottlenecking order fulfillment with manual reviews.
» The threat of being labeled a “high risk” merchant.

While fraud teams focus on fighting waves of new fraud, innovation teams on the other side of the organization are focused on creating new revenue streams, and keeping up with changing customer expectations.

As the decade nears its close, merchants are trying to solve for risk and business opportunity at the same time, and they’re building bridges across their organizations to have big conversations. In this ebook, we’ll try to move the conversation forward.

Read on to discover:

» The most pressing trends in business and fraud that are shaping the future of retail.
» Success stories of customers who have innovated their fraud detection systems with Fraud Detect®, a comprehensive fraud detection solution utilizing a machine learning platform.
» Actions merchants can take now to be proactive in a changing world.
Chapter 01

MERCHANDS ARE EVOLVING THEIR BUSINESS MODELS

Shopping is about to get interesting. If merchants have learned one thing in the past few years, it is customers are clamoring for continuous innovation.

51% of surveyed shoppers last year told Deloitte that they planned to do more holiday shopping online than in stores.²

$2.6 billion
The biggest shopping day last year was not Black Friday, but Cyber Monday – and a third of the $6.6 billion consumers spent that day was via mobile phones.³

$500 billion
The volume of payments via wearables is expected to exceed $500 billion by 2020.⁴

The North Face spent one year training the AI algorithm behind its “Expert Personal Shopper” so it could make recommendations about clothing for consumers.⁵

Now that Amazon’s 20-year patent on 1-click payments has expired, merchants are looking for ways to capitalize on fast payments. Shopify Pay found that increasing checkout speeds by 40% led to an 18% higher conversion rate for returning shoppers.⁶
The latest innovations in commerce are exciting for customers, but they also bring on unique and new challenges when it comes to fighting fraud. Merchants have to get creative to remain competitive.
Email selling
Twenty years after Amazon patented 1-click orders, and two years after social media companies like Pinterest introduced instant “buy” buttons, merchants are looking for the next trend in instant payments.

For example, the startup Rebel is trying to turn email into a merchant-owned channel by enabling customers to make purchases from inside their emails, rather than having to click through to a web browser. Making it easier for customers to complete purchases can create a great customer experience and increase revenue.

Cross-channel shopping
"Omnichannel" has gone from a differentiator to a given in just a couple years. Merchants are searching for ways to integrate all their channels to provide seamless movement between them. According to Google, 65% of people shopping online will begin a purchase with one device but complete it within another.8

Merchants aren’t just integrating digital channels, but physical channels too. For example, Commerce newcomers like Bonobos and MM. LaFleur are expanding their online presence into showrooms, so users can use physical stores as part of their buying journeys.

Voice-based shopping
Thanks to voice selling, Amazon’s Alexa could create $10 billion in revenue by 2020.7 And now that Target and Walmart have partnered with Google to allow voice shopping through Google Assistant, voice computing has become an important new revenue platform – but only for a select few of the most giant merchants.

Small and mid-sized merchants might be shut out of the voice platform for now, but they can optimize their SEO for voice so they show up on searches over voice assistants.

Voice-based shopping
Thanks to voice selling, Amazon’s Alexa could create $10 billion in revenue by 2020.7 And now that Target and Walmart have partnered with Google to allow voice shopping through Google Assistant, voice computing has become an important new revenue platform – but only for a select few of the most giant merchants.

Small and mid-sized merchants might be shut out of the voice platform for now, but they can optimize their SEO for voice so they show up on searches over voice assistants.

IoT is here to stay
The Internet of Things has gone from a buzzword to a Commerce reality. For example, Brita Water is connected to Amazon’s Dash Button and orders new filters automatically when they’re needed. And HP might be resuscitating its lagging printer business in part thanks to Instant Ink, which monitors printer ink levels and sends customers new cartridges before they run out.11

Wallets
In-store mobile payment volume is anticipated to grow from $75 billion in 2016 to $503 billion in 2020.9 Mobile wallets accounted for almost a third of Starbucks transactions last year!10 Wallets can improve the merchant-customer relationship by providing an easier way to pay and a new avenue for personalized promotions. For example, Starbucks “cracked the code” of wallets by offering irresistible enticements through its mobile app, like the capability of ordering coffee ahead of time to skip the line in the store.
Chapter 02

FRAUDSTERS ARE EVOLVING THEIR BUSINESS MODELS TOO

Merchant fraud used to be simpler: someone waiting in line at the return counter with an item they stole. Today, merchant fraud is part of a teeming, underground economy of coordinated financial crime. Fraudsters are leveraging every tool at their disposal to steal from merchants. They’re using advanced technology and leveraging the complexity of the payments ecosystem itself.

Perhaps the most important tool that fraudsters leverage is adaptation. The signature characteristic of today’s financial crime is that it’s always evolving. Here’s a look at the most pressing fraud types and techniques, many of which didn’t even exist a decade ago.
<table>
<thead>
<tr>
<th>FRAUD TYPES</th>
<th>FRAUD TECHNIQUES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Triangulation fraud</td>
<td>Bot attacks</td>
</tr>
<tr>
<td>Here’s how this works: a fraudster sells legitimate products over an auction account, like eBay, and a customer buys the product. The fraudster receives the money, then orders the same item from a legitimate retailer, pays for it with a stolen card, and ships the item to the buyer. The fraudster gets the money, the customer gets the product, and the retailer sees a normal-looking order. It’s only when the chargeback comes a few months later from the victim of the stolen credit card that the retailer discovers the scam.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fraudsters create customized bots, often with the help of &quot;build your own bot&quot; websites, that use programming scripts to choose products at merchants and try to buy them with a velocity that’s not humanly possible, using stolen credit card information. Feedzai has discovered bots that can add to carts five times faster than humans, and bots can be programmed to open fraudulent accounts as well. These bot attacks are concentrated on items that are on sale, have just launched, or are particularly easy to sell.</td>
</tr>
<tr>
<td>Sleeper fraud</td>
<td>Address malformation fraud</td>
</tr>
<tr>
<td>This is a kind of first-party fraud, when criminals open accounts in bad faith using their own identities or creating fictitious ones. In sleeper fraud, criminals will try to simulate normal profiles for months or even years to fool fraud controls. They may even create fake social media accounts associated with these fictitious identities to increase the air of legitimacy. Then they’ll switch their behavior to fraud in an instant.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When a fraud system detects and blocks a fraudulent address, fraudsters will outsmart the fraud controls with a “malformed address.” They’ll write the address in such a way that the system can’t detect (e.g., “R0ad” instead of “road”), but in a way that the human delivering the package will still be able to recognize.</td>
</tr>
<tr>
<td>Chargeback fraud</td>
<td>Prefix phone pattern fraud</td>
</tr>
<tr>
<td>Here a customer will intentionally request a chargeback on a legitimate purchase. The customer might say the item wasn’t delivered, the item isn’t as advertised, the item was returned without a refund being processed, or they don’t remember making the purchase. In friendly fraud, customers will make disputes like these, but because they genuinely are mistaken about the purchase, or possibly because someone in their family made the order without telling them.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fraudsters will “spoof” local area codes in order to look legitimate. They’ll imitate local merchants and fool unwitting customers into giving their personal information. Fraudsters use this same technique to impersonate the IRS and scare people into betraying their own credentials over the phone.</td>
</tr>
<tr>
<td>Reshipper fraud</td>
<td>Synthetic ID fraud</td>
</tr>
<tr>
<td>This criminal enterprise is run by an operator who recruits unwitting “reshipping mules” through work-at-home job scams. They’re promised thousands of dollars a month just to receive and reship packages. The operator sells access to his mules to card thieves, who use stolen card information to purchase products from merchants, ship them to the mule’s address, and have them reshipped. The card thieves sell the goods on the black market, and the operator receives a cut.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identity thieves create new identities using a combination of real and fabricated information. For example, many will use the social security numbers of children to evade discovery. Fraudsters will also fabricate entirely fictitious information. They’ll nurture these identities to appear legitimate, for example, by creating fake social media accounts. And they’ll use these identities to steal lines of credit, open fake accounts, and steal goods.</td>
</tr>
<tr>
<td>Buy online pick up in store fraud</td>
<td>Offline fraud</td>
</tr>
<tr>
<td>Fraudsters will select this option at online checkout, and then call the merchant asking to have it shipped to them after all. This is a way for fraudsters to bypass fraud screens, because merchants consider in-store pickup orders less risky. Fraudsters also like committing this kind of cross-channel fraud because they count on merchants keeping separate, siloed systems for internal and online purchases. For example, an in-store employee may not see that a customer bought 20 of the same item with 20 different identities.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>How can it be possible to see a charge you don’t recognize when the card was in your possession the whole time? Fraudsters can easily buy a small device that clones your card in a moment. They’ll clone your card into a copy that looks just like the real thing, and use it at points of sale to steal from your line of credit or your debit account.</td>
</tr>
</tbody>
</table>
Key data breaches and credential dumps that are fueling all this fraud.

As cybercrime has evolved into big business, data breaches are increasing in both size and impact, disrupting organizations and lowering consumer confidence.

1 BILLION
ACCOUNTS COMPROMISED
Yahoo! data breaches of 2013 and 2014\textsuperscript{13}

100 MILLION
ACCOUNTS COMPROMISED
Linkedin data breach of 2012\textsuperscript{14}

1.4 BILLION
STOLEN CREDENTIALS
discovered by the security firm 4iQ in 2017\textsuperscript{15}
A closer look at the evolving tactics of ATO fraudsters.

At Feedzai, the fraud analyst Joel Carvalhais analyzed the evolution of a fraud ring that attacked a large commerce client with account takeovers (ATO). ATO fraud is growing rapidly, costing $2.3 billion in 2016 alone. When Aite asked financial institutions to name their biggest fraud investment priority, their top answer was: retail ATO.

Feedzai’s analysis demonstrates this ring of ATO fraudsters evolved their tactics in three stages in order to evade detection.

**STAGE 1**

Fraudsters used stolen credentials from the Yahoo! and LinkedIn data breaches to take over customers’ PayPal accounts to steal their card information. Then they used the same stolen credentials to log into the merchant. Fraudsters targeted a whitelist of “good customer” accounts that were auto-approved for orders. They ordered goods under these customers account and sent them to reshipper addresses.

**STAGE 2**

Fraudsters tried to appear legitimate by changing the billing address field to match the shipping address of reshippers.

**STAGE 3**

Fraudsters began to modify every major account field, like username and email address, in order to appear even more legitimate and outsmart the merchant’s rules.
Rules can be effective for stopping certain known behaviors, but rules can reach their limit when it comes to imagining adaptive human behavior.

A model-based approach can uncover interactive relationships in data that rules and humans alone will miss. And unlike rules, models can account for changing human tactics as fraud behavior evolves.

First Data has been deploying Fraud Detect, its machine learning-based fraud detection platform, with national merchants, and the results are in. By combining machine learning models with the existing rules, its customers are increasing fraud detection without adding any friction or alarm.

This adaptive fraud-fighting technology doesn’t just stop criminals in their tracks. It also enables cross-functional innovation efforts to explore new business opportunities without incurring new risks.

Legacy technology simply can’t detect these newer forms of fraud.
1 CASE STUDY: Petroleum Company

Petroleum customer solves fraud crisis resulting from new mobile app

PROBLEM:
When a leading petroleum merchant launched a new mobile application, fraud rates spiked at 32%. This customer faced a critical choice: get fraud under control, or shut down the app and lose out on the new business opportunity.

SOLUTION:
First Data deployed its Premium offering of the Fraud Detect platform, with a customized machine learning algorithm and an advanced case manager. This product is purpose-built for high-touch, high-risk, immediate fulfillment sales.

Use case: Fraud Detect® mobile application

- Mobile App deployed with minimal fraud controls, fraud rate spikes at 33%
- Engaged First Data® to deploy Fraud Detect
- Machine learning models deployed in February '17
- Interim strategy deployed to create 50 sophisticated rules to suppress fraud.
- Three full time fraud analysts. October '16
- Implemented device fingerprinting in late September '16
- FRAUD RATE CURRENTLY AT <0.1%

Data defined as the aggregate amount of chargebacks by original transaction date divided by total number of transactions for a specific month.
CASE STUDY: QSR Company

QSR customer upgrades their fraud detection to enable a new mobile application launch

PROBLEM:
When this customer launched a new version of their mobile app, they saw fraud spikes that called for new tools.

SOLUTION:
The Advanced offering of Fraud Detect was implemented with a machine learning QSR-industry model, a rules engine, and Case Manager. First Data also implemented a capability allowing this customer to test the model at different scoring thresholds.

RESULTS:
- 80% decrease in fraud.
- $200K saved after fees.
A flood of fraud followed a new wallet launch

PROBLEM:
A QSR customer launched an auto-reload wallet. Gift card fraud poured in, along with an unusual volume of balance inquiries on stored value cards. Criminals were launching account takeovers, using stolen credentials to access stored value accounts and purchase items fraudulently.

SOLUTION:
A global model was delivered via a First Data gateway and auto-reload host.

RESULTS:
20,000 fraudulent transactions blocked in the first month alone.
Chapter 04
ACTIONS MERCHANTS CAN TAKE NOW

The half life of innovation is decreasing.

BUSINESSES AND FRAUDSTERS ALIKE ARE CHANGING IN A NEW DIGITAL ECONOMY.
FOR MERCHANTS WHO WAIT TO UPDATE THEIR LIMITED, EXISTING TECHNOLOGY, THINGS ARE ONLY GOING TO GET WORSE – NOT BETTER.

Here are five actions we recommend taking to get ready for a new decade of both risk and opportunity.

1. **Have big conversations across your organization**
   Fraud teams and business teams have never been so linked. In large organizations, it can take a concerted effort to start having meaningful, ongoing conversations about the interconnected effects fraud and new business have on each other. For example, new fraud tools will need to be integrated seamlessly with new products so they don’t add friction. And new business explorations will need to account for the explorations of new fraud tools. Merchants should start operationalizing these conversations as soon as they can, so they can transform their mode from reactive to proactive.

2. **Have big conversations across fraud teams, too**
   Even among fraud teams, silos can exist. For example, digital fraud teams and in-store fraud teams will sometimes work in isolation. Cross-channel fraudsters will quickly discover these organizational communication gaps and find ways to outsmart disjointed fraud teams.

3. **Begin investing now in machine learning**
   A hybrid approach to fraud detection, which combines machine learning models and rules, will identify many more fraudulent transactions for a given alarm rate. Merchants who continue to rely on rules alone will be lapped by today’s fraudsters. Rules provide a static approach to dynamic human behavior, because their thresholds cannot change over time. For example, a human fraudster will quickly discover a velocity threshold for a rule that says, “Block when greater than four transactions in a 30 minute period.” Also, rules can be limited by yes-or-no threshold ranges, whereas models can recommend a broader range of actions, depending on the merchant’s tolerance for risk.
4. **Think “fast”**
In this changing world, speed is king. Merchants need to prioritize speed as a goal in order to outpace the rapid progression of today’s fraudsters. For example, they need to consider how quickly their machine learning system can allow for the training and deployment of new models. And merchants should consider how quickly a vendor can be up and running so they begin stopping new fraud as soon as possible.

5. **Make your people better**
The most fundamental benefit of machine learning is that it makes humans better. For example, while rules can only make a “yes or no” decision about transactions, machine learning models can provide a range of possible actions based on customized risk thresholds. This arms manual reviewers with all the information they need to make a decision, and leaves the power in their hands. Merchants should seek machine learning systems empowering their fraud teams to make informed decisions. Additionally, merchants should seek systems with easy-to-use human interfaces, like drag and drop dashboards and intuitive case managers.
Conclusion

MEET FRAUD DETECT

First Data’s Fraud Detect Solutions is a comprehensive, state-of-the-art fraud prevention solution with real-time fraud scoring and machine learning capabilities.

Designed to reduce a merchant’s overall exposure to and cost of card-not-present payments fraud, Fraud Detect provides a highly differentiated value by leveraging leading-edge technology, the company’s information assets, and global distribution. Fraud Detect has been developed in partnership with Feedzai, an industry-leading AI technology and fraud science company specializing in real-time, machine-based learning to analyze big data and minimize risk in the financial industry.

Fraud Detect is designed as an offering to a merchant who is exposed to the growing fraud threats in eCommerce and card-not-present channels. The underlying objective is to create a centralized solution meeting the very high expectations of retailers for system accuracy, performance and flexibility.
The success of Fraud Detect is tied to three key business objectives:

» Reduce potentially fraudulent transactions, thereby reduce chargeback activity.
» Improve customer satisfaction by reducing false decline rates.
» Improve the efficiency of resources dedicated to managing at-risk transaction case reviews.

With Fraud Detect, merchants can successfully address issues surrounding fraudulent transactions, reducing the number of flagged orders requiring review and significantly lowering false positive rates. Fraud Detect adapts to newer fraud patterns with greater agility through a fully integrated modeling and run-time environment.

Unlike traditional rules-based solutions relying on hard-coded rules thresholds, the machine learning platform uses profiles to compute thresholds that are updated with each incoming transaction as it happens. The merchant is afforded access to a single fraud prevention solution, including both rules engine and machine learning, to make payment and operations safe across all channels.