Attack rate increased moderately over 2016

Holiday surge in US: domestic orders in Q4 2016 were 79% riskier than in Q4 2015

Attacks against Apparel rose 69.9% over 2016

Attack Methods Analysis (see page 20)

Despite a 16% decline in ATO (Account Takeover) on merchant website accounts, Account Takeover on Online Payments accounts (e.g. PayPal) spiked by 131%.

Domestic / International Analysis (see page 5-9)

• Domestic orders spiked, reaching a peak of $4.98 at risk per $100 of sales in Q4 2016 (compared to $2.7 in Q4 2015).

• International risk remained high: 62.4% riskier than domestic.
**2015 | 2016 Attack Rate Industry Trends**

- **Luxury**: 8.4% ↓
- **Electronics**: 1.8% ↓
- **Apparel**: 69.9% ↑
- **Travel**: 33% ↓
- **Digital goods**: 22.6% ↓
- **Food & beverages**: 49.8% ↑

*Yearly average comparison of dollars at risk per $100 of sales during 2016 compared to 2015. Dollars at risk represent both successful and unsuccessful fraud attacks. See pages 12-17 for full data.*
The Forter/MRC Fraud Attack Index

Constant change and continual development characterizes today’s online fraud ecosystem. Fraudsters are creative, agile and have easy access to a wider range of tools and data than ever before.

Online criminals are always looking for new ways to commit successful theft, and they’re becoming increasingly sophisticated in their methods, leveraging automation to widen their scope and scale, researching their victims (especially those affected by account takeover), and exploring ways to exploit new payment methods.

Against this background, it is increasingly vital for fraud prevention professionals to have a clear understanding of the trends and movements in the world of online fraud. To combat these criminals effectively, it is important to know how they’re working, what they’re doing and where they’re attacking.

Forter and MRC have created this Fraud Attack Index in order to reflect these changes as they affect US e-commerce and mobile merchants and to provide antifraud professionals with the context they need to succeed.

This report examines the trends in online fraud attacks across industries, comparing the different situations experienced by different industries. It also compares domestic to international attacks, by country of payment instrument issuance.

The report also looks at the trends in the usage by fraudsters of specific methods or directions of attack (e.g. location manipulation, account takeover, etc.). This is to provide insight into the various techniques commonly employed by today’s savvy fraudster.

The increased sophistication of the online criminal underworld, where a huge and connected marketplace exists to provide numerous services that make theft easier (and where stolen data can be found easily and cheaply following the massive data breaches of the last few years), means that fraudsters have direct access to the tools and information they need to commit online fraud. This has lowered the barrier to entry for new fraudsters to enter, and enabled experienced fraudsters to increase the scale, sophistication and speed of their attacks.

This report is designed to reflect the current patterns in that scene and help merchants to understand further and prepare for the attacks they are seeing or are likely to face.
Online Fraud Attacks in 2016

Overall, 2016 saw a steady rise in online fraud attack rate, which increased 8.9% over the course of the year. The frightening “tsunami” of fraud attempts that many merchants experienced at the end of 2015 was not repeated, but the moderate rate of increase was sustained. For several industries, primarily apparel, digital goods and travel, 2016 was a year of dramatic fluctuations, affected by numerous fraudsters who were looking for new vulnerabilities they can exploit.

This may be because the fraudster community had shifted online in advance of and directly after the US adoption of EMV, knowing that card present fraud would be more difficult and that the card not present channel would be more vulnerable. Once that initial move had been made, the trend continued upwards but was not marked by a remarkable increase in the same way since the main shift had been completed.

The general increase in fraud attack rate reflects the appealing nature of the online channel to the criminal community. The growth of e-commerce and mobile commerce, the abundance of stolen data, the opportunities for obfuscation, the tools available to them, the unlikelihood of reprisals for fraud attempts and more all combine to make online attacks attractive to criminals.

Within that trend, some industries are more attractive than others. Luxury goods continue to be highly sought after by fraudsters, with an average fraud rate of $5.91 at risk out of $100 of sales, which is 41% higher than electronics. However, during 2016, there was also a 69.9% rise in the attacks against Apparel websites and goods, as this industry came under attack more than ever before, partially attributed to serial liar-buyer abuse, in addition to traditional stolen-CC fraud.

Domestic orders have shown a notable rise in fraud attack rate, becoming 79% riskier than they were in 2015. This has had a direct impact on the bottom line risk, resulting in a shift from $2.7 at risk per $100 of sales in Q4 2015, to $4.98 in Q4 2016.

International orders (where the payment instrument is outside the US) remain more fraudulent than domestic. While the extent to which this is the case varies by industry, the trend is consistent throughout industries. Overall international orders are 62.4% riskier than domestic ones. Cross-border commerce is an increasingly significant source of revenue for many merchants, so it is important to be aware of the risks as well as the advantages attached.
Domestic Online Fraud Attacks

The rise of domestic online fraud attacks is one of the most notable features of the 2016 results. Comparing the rate of attack in Q4 2015 to the rate in Q4 2016 shows that online attacks have almost doubled for domestic orders.

Quarterly Breakdown of Attack Rate 2015-2016:
US Domestic Fraud Spiked During The Holidays

[Graph showing quarterly breakdown of attack rate with data points for 2015 and 2016, indicating a spike during the holidays.]

The question of why domestic attacks in particular have risen is an interesting one, and it may well be one of the consequences of EMV adoption in the United States.

Vertical Breakdown of US Domestic Quarterly Attack Rate 2015-2016:
Apparel in particular has shown a dramatic increase in attack rate

[Graph showing vertical breakdown of US domestic quarterly attack rate with data points for apparel in 2015 and 2016, indicating a significant increase in Q4 2016.]
Since microchip cards make card present so much harder for American fraudsters, those forms of fraud have become less prevalent. In fact, MasterCard reported as early as January 2016 that they had seen a 27% reduction in counterfeit fraud (by dollar volume), as compared to the same period last year.¹

It is domestic fraudsters who are hardest hit by EMV, and the most natural move for them to make is to online card not present transactions. It was predicted well in advance of the adoption deadline that CNP transactions would suffer from EMV, and it appears that this is indeed what has happened. Naturally, EMV isn’t the sole factor behind the fluctuations of 2016 and it should not be used as a single explanation for all of them. The true picture of fraud risk is always fluid and sensitive to a complex combination of factors. The specific relevant combination is often unique for each industry, if not for each online merchant.

¹http://www.nacsonline.com/Media/Daily/Pages/ND0531163.aspx#Win88ht96uV
International Online Fraud Attacks

In terms of overall trend, international online fraud attacks mirror the domestic pattern, with numbers going up overall and showing some seasonal variation during the Q4 periods.

**Quarterly Breakdown of Attack Rate 2015-2016:**
The “Fraud Tsunami” of 2015 is winding down, and the average international risk rate remains 2.5 times higher than the US domestic risk rate.

The same trends can be seen in terms of industry breakdown, with luxury and digital goods continuing in fraudster popularity and fashion becoming increasingly popular.

**Vertical Breakdown of International Quarterly Attack Rate 2015-2016:**
Apparel, in particular, has shown a rise in fraud attack rate.
What is notable about the international online fraud attacks is that the rate is on the whole so much higher than the domestic rate. In fact, international orders are 63% riskier than domestic ones. This is the case despite the fact that international fraud attacks have actually decreased 13% in comparison to 2015.

While a high risk of fraud is not necessarily unexpected for international orders, it reinforces the need for fraud systems and teams to be aware of the geographical elements in a transaction and invest in understanding how different combinations of location may impact what can be known about the nature of the transaction.

Research into and a deep understanding of the idiosyncrasies of any international markets that are particularly pertinent to the business will assist fraud departments to avoid both international fraud and international false positives.
Domestic / International Comparison

Although the domestic attack rate has increased dramatically, almost doubling between Q4 2015 and Q4 2016, international fraud attacks remain considerably higher than domestic.

Domestic and International Attack Rate ($ at risk out of $100 of sales)

This is the case overall, and also when considering each industry separately, meaning that regardless of the vertical in which they operate, merchants with an online presence must be aware of the risks of international orders and ensure their fraud prevention systems are able to deal with this threat effectively without increasing false positives through over-caution.
Domestic / International Industry Comparison

Within this context, the trends that are notable on the domestic level are even more pronounced internationally.

At its peak, the luxury goods online fraud attack rate was more than three times the domestic rate.

Luxury Goods Domestic and International Attack Rate ($ at risk out of $100 of sales)

Apparel Attack Rate
Quarterly Breakdown: Domestic & International
Considering the 2016 fraud attack rate in comparison to 2015, we see that 2016 also represents a general increase. Overall, over the course of the year, we see a moderate 8.9% increase in fraud attacks.

**Breakdown of Domestic / International Quarterly Attack Rate 2015-2016:**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>0</td>
<td>4.3</td>
<td>0</td>
<td>8.1</td>
</tr>
<tr>
<td>Q2</td>
<td>0</td>
<td>2.2</td>
<td>0</td>
<td>8.8</td>
</tr>
<tr>
<td>Q3</td>
<td>0</td>
<td>3.4</td>
<td>0</td>
<td>8.1</td>
</tr>
<tr>
<td>Q4</td>
<td>0</td>
<td>2.9</td>
<td>0</td>
<td>8.1</td>
</tr>
</tbody>
</table>

**Overall Average Attack Rate Quarterly Breakdown**

<table>
<thead>
<tr>
<th>Quarter</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>7.2</td>
<td>5.5</td>
</tr>
<tr>
<td>Q2</td>
<td>6.4</td>
<td>6.6</td>
</tr>
<tr>
<td>Q3</td>
<td>6.6</td>
<td>5.1</td>
</tr>
<tr>
<td>Q4</td>
<td>6.1</td>
<td>6.6</td>
</tr>
</tbody>
</table>

8.2% Holiday increase over Q4 2015
Online Fraud Across Industries

2016 saw a slow but steady increase in fraud attacks for e-commerce as a whole. The rate fluctuated over the course of the year and varies dramatically between industries and individual merchants.

While the slight increase is constant over the year, there is a small spike over the Q4 holiday period as fraudsters capitalize on the festive shopping rush to hide their activities. In this sense, 2016, like 2015, challenged the traditional conviction that fraud rates are always drowned by good traffic in the holidays.

Industry Breakdown of Domestic Quarterly Attack Rate 2015-2016:

![Bar chart showing domestic quarterly attack rate for different industries]

Industry Breakdown of International Quarterly Attack Rate 2015-2016:

![Bar chart showing international quarterly attack rate for different industries]
Apparel

The most notable growth in fraud attack rate is within the Apparel industry. Comparing the rate in Q4 2016 to that of Q4 2015 shows a significant increase of 69.9%.

This may be related to the new fraudsters who have joined the online criminal community following EMV adoption in the US, who are perhaps sticking to a vertical they understand. It may also reflect the increased comfort of genuine shoppers with the idea of buying fashion items online and returning as necessary.

Apparel has traditionally been a lower risk vertical (compared to, say, luxury or digital goods), so it may be that these merchants have been more relaxed than those in industries known to be high risk. The danger is that this approach can lead to complacency, so that merchants are less likely to invest in keeping ahead of fraud trends. When the fraudster community discovers a vulnerability, the industry is less prepared to counter the threat and the criminals zero-in on this weakness. This kind of situation may have influenced the spike over 2016.

Another notable spike of attacks against Apparel occurred during Q4 2016. This was probably in part because these goods are popular as gifts during the holidays and fraudsters were counting on this trend to help cover their actions. However, since other holiday gift industries did not experience the same level of attack, it may be that the Q4 spike was influenced by a group of abusers or fraud ring who found a lucrative vulnerability in some fashion websites during Q3, and returned en masse during the holidays.

Apparel Attack Rate ($ at risk per $100 of sales)
Luxury Goods

The fraud attack rate remained almost flat within the luxury goods industry, and still considerably higher than most other physical goods. This is understandable given that this industry possesses characteristics that make it especially attractive to online criminals. Luxury in 2016 showed a very mild 8.4% decrease in fraud attack rate, indicating that this industry’s popularity with the criminal community is hardly impaired.

While merchants are generally particularly cautious about approving high value orders, when fraud is successful the ROI for the fraudster is high since the items are valuable and, given their popularity, fairly easy to resell. For this reason they keep on coming, even if their fraud is foiled time and again.

The mild dollar-value decrease in attack rate during 2016 is also explained by the fact that fraudsters have increasingly been targeting mid-range luxury goods, knowing that it is easier to slip under the radar with these goods which are scrutinized less closely, and knowing that there is a large market of buyers willing to purchase such items at slightly less than the usual cost.

Luxury Goods Attack Rate ($ at risk per $100 of sales)
Digital Goods

As usual in this highly unstable category, attack rates have shifted dramatically throughout the year. Measuring fraud in digital goods is particularly tricky because of the highly trend-sensitive nature of the industry.

As shown below, a fraud surge around the holiday season of 2015 was uncharacteristic, and indeed can mostly be attributed to a dominant fraud trend in the gaming community. During 2016 this trend petered out and attack figures in Q4 represent the calmer period of the holidays, when many gift card websites enjoy a wave of good traffic, and fraudsters who are shopping for their “business” (e.g. buying hosting services to help them conceal geolocation) are much less active.

Digital Goods Attack Rate ($ at risk per $100 of sales)
Quarterly Breakdown: Domestic & International
Travel & Hospitality

The always erratic business of travel, which traditionally suffers almost equally from fraud risk and from buyer’s remorse, was among the most popular fraud scenes during 2015. In this context, 2016 presented milder fraud figures, with overall 33% lower attack rates throughout the year.

While the calmer fraud rates in this industry should encourage travel agencies to focus on legitimate traffic and business enablement, a word of caution is due regarding the increasingly frequent use of US credit cards in travel fraud attacks during 2016. The trend is partially attributed to the use of US-issued prepaid cards (funded by stolen payments instruments), as well as middle-man schemes, where an airline/travel-merchant is being fooled by a fraudster claiming to be a travel agent and ordering travel services in bulk.

Travel & Hospitality Attack Rate ($ at risk per $100 of sales)
Quarterly Breakdown: Domestic & International
Food Deliveries

2016 witnessed a dramatic and consistent 49.8% increase in fraud rates for food deliveries (as well as takeaways and some grocery vendors). However, since the majority of the increase occurred with international payment instruments, the fraud trend does not necessarily indicate a genuine spike in fraudsters’ appetite for this industry. It is more likely that the increasing use of foreign stolen payment instruments for food purchases has become a popular way for fraudsters to test their payment credentials before they initiate a more sophisticated attack on other industries. Also, keep in mind that most food delivery merchants who were included in this segment for 2016 do not cater to international orders, which also correlates with the fact that most international traffic to their website is fraudulent.

Food Deliveries Attack Rate ($ at risk per $100 of sales)
Quarterly Breakdown: Domestic & International
Methods of Attack

The methods of attack favored by the online fraudster community show variation over time. In part this is because these criminals, who are by nature creative and always looking for new vulnerabilities and ways to steal successfully, continually develop new tools and techniques.

Since the figures in this report represent both successful and unsuccessful attacks, it is very rare to see any type of attack method disappear completely from the map (because there’s always a new fraudster who’s going to try account takeover, for example, even after the merchant has built up anti-ATO protections). Eventually, most fraudsters will despair after striking out several times and will move on, either to a different online store or (less frequently) to a different attack method.

Effective new fraud methods will be popular for some time, while fraud prevention departments struggle to catch up, and then fade in popularity as new ways are found to detect or block them - until a new version is developed that out-maneuvers those defensive measures, and so on.

Fraudsters also adapt to changing trends in the e-commerce and payments spheres. For example, new payment methods are examined for weaknesses which are exploited if found, new buyer trends such as the move to omnichannel may be used for concealment or as the basis for a new kind of attack, and so on.

Attack Methods Quarterly Breakdown of Attack Rates ($ at risk per $100 of sales)
### Attack Rates by Method of Attack (average dollars at risk per $100 of sales)

<table>
<thead>
<tr>
<th></th>
<th>Repeating Offenders</th>
<th>Location Manipulation</th>
<th>Account Takeover</th>
<th>Online Payments</th>
<th>Botnets and Virtual Machines</th>
<th>Food Deliveries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1-15</td>
<td>4.86</td>
<td>5.97</td>
<td>0.83</td>
<td>1.03</td>
<td>9.5</td>
<td>3.73</td>
</tr>
<tr>
<td>Q2-15</td>
<td>4.88</td>
<td>6.7</td>
<td>1.02</td>
<td>1.02</td>
<td>12.8</td>
<td>5.33</td>
</tr>
<tr>
<td>Q3-15</td>
<td>3.27</td>
<td>5.53</td>
<td>8.9</td>
<td>2.25</td>
<td>17.4</td>
<td>2.03</td>
</tr>
<tr>
<td>Q4-15</td>
<td>1.94</td>
<td>3.27</td>
<td>10.2</td>
<td>0.25</td>
<td>11.8</td>
<td>1.08</td>
</tr>
<tr>
<td>Q1-16</td>
<td>2.91</td>
<td>5.62</td>
<td>9.79</td>
<td>0.2</td>
<td>3.13</td>
<td>3.02</td>
</tr>
<tr>
<td>Q2-16</td>
<td>4.48</td>
<td>4.52</td>
<td>2.32</td>
<td>1.85</td>
<td>4.31</td>
<td>3.48</td>
</tr>
<tr>
<td>Q3-16</td>
<td>3.74</td>
<td>4.77</td>
<td>2.15</td>
<td>2.7</td>
<td>3.45</td>
<td>2.53</td>
</tr>
<tr>
<td>Q4-16</td>
<td>4.79</td>
<td>3.92</td>
<td>3.72</td>
<td>5.74</td>
<td>4.08</td>
<td>2.64</td>
</tr>
</tbody>
</table>

### Methods of Attack (by relative share in attack rate)

- **2015**
  - Online Payments: 76%
  - Location Manipulation: 11%
  - Account Takeover: 14.5%
  - Identity Theft: 18.7%
  - Repeating Offenders: 20.2%
  - Botnets and Virtual Machines: 27.9%

- **2016**
  - Online Payments: 11.6%
  - Location Manipulation: 12.9%
  - Account Takeover: 16.5%
  - Identity Theft: 17.4%
  - Repeating Offenders: 20.5%
  - Botnets and Virtual Machines: 21%
Account Takeover (ATO) and Online Payments Takeover

A growing recent trend in the realm of account takeover (ATO) is the use of hacked online payment accounts such as PayPal, ApplePay, AndroidPay etc. In these attacks the fraudster breaks into the victim's account and uses the details there, including payment details, to make purchases and take actions as if they were the victim.

From the fraudster perspective this is an excellent arrangement since it smooths their path (difficulties with authentication, money in account, etc. are much reduced) and means that their attempt seems more legitimate and is more likely to be approved. For this reason, it became more important for merchants to have good defences against this kind of ATO in particular during 2016.

The unprecedented data breaches of the last few years have included account and password information and this, combined with the fact that many consumers continue to reuse passwords across multiple accounts, has made this form of attack easier to carry out.

Interestingly, while 2015 showed a rise against accounts belonging to merchant sites, in 2016 we have seen this trend decrease. It has been supplanted instead by a rise in ATO attacks against online payments in particular. This may reflect increased general usage of such alternative payment options, and certainly it is understandable from the fraudster's perspective since breaking into the payment method itself increases the scale and range of theft available to them.

ATO and Online Payments Quarterly Breakdown

![ATO and Online Payments Quarterly Breakdown Graph]
**Note on Botnets**

In general, botnets are popular within the fraudster community because they increase the scale and reach available to the criminal. There was a significant spike in the use of botnets during 2015, when this technology became widely and easily available even to fraudsters without notable technical knowledge or ability.

However, Forter’s data showed considerably less botnet activity in 2016, which is believed to be skewed due to Forter’s unique anti-fraud technology (Simply put: we’ve practically chased the botnet fraudsters away, so our measurements of their activity during 2016 are unlikely to be representative). Forter is aware that the proprietary technology used in-house to detect and block botnets is more sophisticated than most fraud solutions available, which suggests that many botnet fraudsters (who were not able to conduct their attacks on Forter’s clients) migrated to other merchants to see if they could operate more easily elsewhere.

This receives mention here because unlike in other areas, where the trends seen within existing customers match those seen with new customers (for example in terms of vertical, attack rate, or other attack methods) the botnet usage trend is somewhat different.

New customers, added during 2016, came to Forter with higher botnet usage but matched the general trend Forter sees with existing clients within a quarter, presumably as the fraudsters had realized that this attack was not working any longer and moved on.

Arising from this are two points. Firstly, and anecdotally, it is interesting to note this example of the adaptability of the fraudster group. They are in this sense “data-driven.” They will try methods and techniques of attacks, analyze their success, and share information about which are successful against a given target. When a previously successful method ceases to be effective, their monitoring picks up this trend and they try something else or try a different target.

This characterizes the “ROI mindset” of today’s fraudsters. Their aim is to minimize effort and maximize profit. To do this they keep close track of what works against which targets. If effort increases or profits decrease, they will move elsewhere. This is, in a way, encouraging for those whose job is to protect their company against fraud.

While this trend is included in this report as being of interest to the intended audience, it may not reflect the experience of other merchants or vendors and so it is flagged here to avoid giving a misleading impression.
Botnets Attack Rate ($ at risk per $100 of sales): 2015 Rise & 2016 Eradication

- Q1: 9.5
- Q2: 12.8
- Q3: 17.4
- Q4: 11.8

- Q1: 3.13
- Q2: 4.31
- Q3: 3.45
- Q4: 4.08

Botnets and Virtual Machines
Methodology

What is the Index?

Forter’s Fraud Attack Index, prepared in conjunction with MRC, measures the growth (or decline) of attempted fraud on US merchant websites. It quantifies the potential cost (if left unchecked) to merchants, based on attack amounts and how these amounts are trending over time.

Index Development

We collected data on the attack rate, aggregated by yearly quarters. The attack rate is defined as the average dollars at risk out of every $100 of sales.

Attack rate was calculated by % of dollar amount in fraudulent orders (both declined orders, where the fraud was mitigated in real-time, and undetected fraud transactions which were later reported), divided by the total sales amount of the respective quarter.

Attack rates were calculated using a variety of merchants, most of whom were veteran customers of Forter. For customers who joined Forter during 2015 or 2016, attack rates were calculated based on historical data provided by the merchant. Forter’s automated fraud algorithm was used to detect fraud patterns in historical transactions in order to calculate fraud MOs in historical data.

For the 2016 H1 Global Fraud Index, by Forter & PYMNTS, see pymnts.com/global-fraud-attack-index/

Segmentation and Breakdown

The following 4 types of segments and breakdowns were applied to allow an analysis of fraud trends:

• Quarterly breakdown - by date of order.

• International vs. US domestic breakdown - by country of payment instrument issuance.

• Industry - by merchant websites (based on the predominant category of item sold on the website, meaning that a website selling mostly cellphones and laptops will be classified as electronics, even though some sales on this website may include accessories).

• MO - modus operandi, meaning method of attack detected (based on Forter’s fraud detection algorithm and not based on merchant report). MOs may overlap, e.g. when a fraudster performs both ATO and location manipulation in a single attack.
Merchant Segments
The following merchant segments were included in the development and analysis of the Fraud Attack Index:

- Apparel: Covers a variety of merchant segments from casual to smarter wear, both clothing and footwear. All merchants in this segment accept international orders. High-end brands would be categorized as Luxury due to differing patterns of fraud.

- Luxury: High-end brand merchandise including clothing, jewelry and accessories (e.g., Rolex, Louis Vuitton, etc.). All merchants in this segment accept international orders.

- Electronics: Direct sellers and retailers of electronic goods, including laptops, tablets, e-readers, smartphones and accessories. All merchants in this segment accept international orders.

- Travel & Hospitality: Airlines, travel agencies, travel search engines, hotel room search engines and travel marketplaces. All merchants in this segment accept international orders.

- Food deliveries: Digital food delivery requests, including restaurant take-aways and grocery deliveries. Most merchants in this segment do not accept international orders.

- Digital Goods: Gift cards, eBooks, music, gaming; also includes business-related virtual services such as hosting and software solutions. Most merchants in this segment accept international orders.

Attack Methods Glossary

- ATO - Fraudster hacked into the account on the merchant’s website (thus passing as a returning customer).

- Online Payment Account Takeover - Fraudster hacked into an online payment service account (PayPal, Apple Pay, Android Pay, etc.).

- Identity Theft - Fraudster used credentials (e.g. e-mail) stolen from a 3rd party or parties.

- Repeating Offender - A fraudster who had previously been spotted at least once making an attempted attack on at least one of Forter’s customers.

- Botnets & Virtual Machines - Fraudster submitted purchase orders using a script or piece of code, often running remotely on a slave machine.
About MRC

With the vision of making commerce safe and profitable everywhere, the Merchant Risk Council is the leading global trade association for eCommerce fraud and payments professionals. The MRC was established in 2000 by a small group of merchant professionals from leading consumer brands who all shared a mutual goal of improving eCommerce payments while supporting their organizations’ risk management efforts. In 2010, the MRC expanded its community to Europe, and currently supports over 450 member companies in over 30 countries.

About Forter

Forter provides fully automated and highly accurate real-time fraud decisions, eliminating rules, scores and manual reviews. That’s an instant approve or decline decision for every transaction, covered by a full fraud chargeback guarantee. We call it Decision as a Service®.

With Forter’s exceptional accuracy, online merchants experience increased approvals, a smoother checkout experience, and the near elimination of false positives - meaning more sales and happier customers at a much lower cost.

Full automation means scale is no longer a problem, even during the busiest of seasons. It removes the InfoSec risk that comes with a reliance on manual reviews and ensures that fraud prevention no longer creates delays on the fulfillment side. Since we charge only for what we approve and offer a chargeback guarantee, fraud management becomes a predictable item for Finance teams as well.

It’s all possible because of our “Integrated Intelligence” - the powerful combination of Artificial Intelligence with the constant research and analysis of our team of human experts. This allows us to maximize the potential of “big data” while also keeping ahead of today’s sophisticated fraudster ecosystem and their new techniques and attacks.

Feedback

We are interested in your feedback on this report. If you have questions, comments, or would like to subscribe to this report, please email us at media@forter.com.