National SME Fraud Segmentation
2012
Contents

- Executive Summary Page 3
- Building the Segments Page 4
- Introducing the Segments Page 13
  - Key segment attitudes
  - Segment dimensions
- Segment Details Page 18
  - Segment A Page 19
  - Segment B Page 26
  - Segment C Page 33
  - Segment D Page 40
  - Segment E Page 47
  - Segment F Page 54
- Communications Strategy Page 61
- Segment Comparisons Page 75
  - Key variables
  - Geo-demographics
- Mapping to the Consumer Segments Page 83
- Appendix Page 89
  - Segment dimension summary
  - The segmentation process
  - Additional data sources
  - Geo-demographic differences
  - SME definitions
  - Fraud type definitions
Executive summary

- This document contains information on the market segments for small and medium sized enterprises (SMEs), based on attitudes and behaviours towards fraud and internet crime.

- 26 qualitative and 2,400 quantitative interviews were undertaken with key SME decision makers exploring how, when and why SMEs fall vulnerable to fraud and internet crime.

- Six distinct SME segments were identified based on an analysis of awareness of fraud, perceived risk and actual risk.

- The segmentation is to be used by the National Fraud Authority (NFA), Department for Business Innovations & Skills (BIS) and their partners for:
  - **Insight and Understanding** of SME fraud and internet crime risks
  - **Prevention Strategies** to help SMEs better protect against fraud
  - **Communications** to target at-risk segments, raise awareness and encourage behaviour change
  - **Measurement** of behaviour change and the impact of campaigns

- The segmentation can also be used by wider public or private sector to append to their own customer data, gain a better understanding of how attitudes and behaviours influence susceptibility to fraud and develop prevention strategies as a solution.
Building the segments
The segments were built using three key dimensions

- **Awareness**: How aware are SMEs of different types of fraud?
- **Perceived Risk**: How at risk of fraud do SMEs think they are?
- **Actual Risk**: How at risk of fraud are SMEs actually?
Factoring in actual risk – 25% surveyed have experienced fraud in last 12 months
We have used a decision tree to identify factors that make businesses susceptible to fraud.

Annual Turnover is important to differentiate.

Online trading influences vulnerability to fraud.

Larger business with more employees are more at risk.

Specific business categories are more at risk.
£20 - £40 million turnover most at risk

There’s a key point in a business’ turnover that makes them more vulnerable – significant increase in risk at £20m+.
Of those experiencing fraud, online traders are more likely to be hit.

11% higher
Fraud experience relates directly to the size of business

- 1 employee (I am the only employee of my company)
- 2 to 5 employees
- 6 to 9 employees
- 10 to 49 employees
- 50 to 99 employees
- 100 to 249 employees

% Experienced Fraud (Last 12 Months)
## High risk areas of business

### Indexing Experience of fraud against average number of employees

<table>
<thead>
<tr>
<th></th>
<th>Account takeover</th>
<th>Card not present</th>
<th>Cheque</th>
<th>Computer Software Service</th>
<th>Computer hacking</th>
<th>Employee assets and inform</th>
<th>Fake invoice scams</th>
<th>Intellectual property and</th>
<th>Identity</th>
<th>Other types of</th>
</tr>
</thead>
<tbody>
<tr>
<td>A - Agriculture, Forestry And Fishing</td>
<td>0</td>
<td>36</td>
<td>0</td>
<td>0</td>
<td>18</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>B - Mining And Quarrying</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>C - Manufacturing</td>
<td>4</td>
<td>15</td>
<td>12</td>
<td>8</td>
<td>37</td>
<td>15</td>
<td>23</td>
<td>19</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>D - Electricity, Gas, Steam And Air</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>12</td>
<td>18</td>
<td>12</td>
<td>12</td>
<td>0</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>E - Water Supply, Sewerage, Waste</td>
<td>7</td>
<td>13</td>
<td>7</td>
<td>7</td>
<td>26</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>F - Construction</td>
<td>22</td>
<td>39</td>
<td>39</td>
<td>31</td>
<td>79</td>
<td>44</td>
<td>44</td>
<td>26</td>
<td>26</td>
<td>31</td>
</tr>
<tr>
<td>G - Wholesale And Retail Trade, Repair</td>
<td>5</td>
<td>60</td>
<td>28</td>
<td>18</td>
<td>55</td>
<td>28</td>
<td>41</td>
<td>23</td>
<td>5</td>
<td>28</td>
</tr>
<tr>
<td>H - Transportation And Storage</td>
<td>6</td>
<td>17</td>
<td>8</td>
<td>11</td>
<td>28</td>
<td>20</td>
<td>14</td>
<td>6</td>
<td>6</td>
<td>14</td>
</tr>
<tr>
<td>I - Accommodation And Food Service</td>
<td>14</td>
<td>57</td>
<td>24</td>
<td>33</td>
<td>38</td>
<td>29</td>
<td>29</td>
<td>19</td>
<td>10</td>
<td>38</td>
</tr>
<tr>
<td>J - Information And Communication</td>
<td>23</td>
<td>55</td>
<td>14</td>
<td>37</td>
<td>142</td>
<td>32</td>
<td>46</td>
<td>46</td>
<td>37</td>
<td>18</td>
</tr>
<tr>
<td>K - Financial And Insurance Activities</td>
<td>16</td>
<td>23</td>
<td>10</td>
<td>7</td>
<td>49</td>
<td>23</td>
<td>16</td>
<td>7</td>
<td>10</td>
<td>7</td>
</tr>
<tr>
<td>L - Real Estate Activities</td>
<td>11</td>
<td>23</td>
<td>17</td>
<td>23</td>
<td>68</td>
<td>6</td>
<td>17</td>
<td>17</td>
<td>23</td>
<td>17</td>
</tr>
<tr>
<td>M - Professional, Scientific And</td>
<td>34</td>
<td>89</td>
<td>55</td>
<td>41</td>
<td>226</td>
<td>62</td>
<td>123</td>
<td>27</td>
<td>55</td>
<td>41</td>
</tr>
<tr>
<td>N - Administrative And Support Service</td>
<td>4</td>
<td>17</td>
<td>9</td>
<td>9</td>
<td>17</td>
<td>4</td>
<td>9</td>
<td>9</td>
<td>13</td>
<td>4</td>
</tr>
<tr>
<td>O - Public Administration And Defence,</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>P - Education</td>
<td>0</td>
<td>15</td>
<td>9</td>
<td>15</td>
<td>29</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td>Q - Human Health And Social Work</td>
<td>9</td>
<td>15</td>
<td>6</td>
<td>6</td>
<td>30</td>
<td>15</td>
<td>18</td>
<td>6</td>
<td>9</td>
<td>18</td>
</tr>
<tr>
<td>R - Arts, Entertainment And Recreation</td>
<td>21</td>
<td>62</td>
<td>21</td>
<td>62</td>
<td>124</td>
<td>34</td>
<td>62</td>
<td>34</td>
<td>41</td>
<td>62</td>
</tr>
<tr>
<td>S - Other Service Activities</td>
<td>31</td>
<td>82</td>
<td>56</td>
<td>77</td>
<td>154</td>
<td>56</td>
<td>92</td>
<td>20</td>
<td>36</td>
<td>56</td>
</tr>
<tr>
<td>T - Activities Of Households As</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>U - Activities Of Extraterritorial</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Indexing type of fraud against business classification – volume of fraud in the last 12 months**
Each quintile is assigned a probability of fraud.

Without a model we expect 25% of respondents to experience fraud.

59% Fraud
30% Cyber fraud

21% Fraud risk
12% Cyber fraud

29% Fraud risk
16% Cyber fraud

36% Fraud risk
19% Cyber fraud

52% Fraud Risk
32% Cyber fraud
Introducing the segments
The three dimensions uncover distinct attitudes between the segments

**Segment A**
We know about fraud and think we can spot it, so it won’t happen to us

**Segment B**
We’re worried about fraud but don’t have the time or knowledge to know what to do

**Segment C**
We don’t need to think about fraud on a day to day basis

**Segment D**
We’ve been hit by fraud but we’ve taken steps to protect ourselves, so we’re safe

**Segment E**
We’ve tried to protect ourselves and it didn’t work so now what do we do?

**Segment F**
Fraud’s inevitable, we’ll deal with it when it happens
Awareness and perceived risk

- **A**: High Awareness - Low Perceived Risk
  - Colour: 0.9%
  - Size of bubble: 4.5m UK SMEs

- **B**: Low Awareness - High Perceived Risk

- **C**: Low Awareness - Low Perceived Risk

- **D**: High Awareness - High Perceived Risk
  - Colour: 1.9%

- **E**: High Awareness - Low Perceived Risk
  - Colour: 0.9%
  - Size of bubble: 4.5m UK SMEs

- **F**: Low Awareness - High Perceived Risk
Awareness and actual risk

At Actual Risk

High Awareness

Low Awareness

Extreme Actual Risk

Colour = % of turnover Lost to fraud
0.9%
1.9%

Size of bubble = count of UK SMEs
(Total = 4.5m)
How the segments map across all 3 dimensions

- **Colour** = % of turnover Lost to fraud
  - 0.9%
  - 1.9%

- **Size of bubble** = count of UK SMEs (Total = 4.5m)

- N.B. % of fraud experienced in the last 12 months can be lower than their actual risk level due to their defences e.g. Under Siege are at the most risk but have only experienced slightly above average % fraud in the last 12 months
Segment details
We’re knowledgeable about fraud and think we can spot it so it won’t happen to us

Segment A’s attitudes come from the fact that although they are highly aware of fraud types, they have had relatively low experience of it. They think their awareness will serve them well in the future to spot and stop fraud, even though this won’t be enough by itself.

“We know a lot about fraud and the methods”

“We fraud isn’t likely to happen to me”
Segment A

- **Key sectors**
  - J - Information And Communication
  - M - Professional, Scientific And Technical Activities
  - N - Administrative And Support Service Activities

- **Key attitudes**
  - Feel they know a lot about fraud and fraudulent methods
  - Think fraud is unlikely to happen at their company
  - Believe they have enough security in place to protect themselves

- **Key actions/inactions**
  - Don’t use consultants for fraud advice
  - Don’t take every precaution as their experience of fraud hasn’t been that serious or widespread

“I can’t see out of the people we work with who would be fraudulent”

“We haven’t done a risk assessment; it would be too large and formalised for such a small business”
Segment A: Key attitudes

% Definitely and tend to agree

- After being the victim of fraud we have put in measures to protect ourselves: 9 (77)
- Fraud is unlikely to happen to my company: 34 (128)
- We know a lot about the methods fraudsters use: 38 (120)
- We would be able to spot a fraud: 48 (114)
Segment A: Fraud experience

All Fraud 19%  |  Cyber fraud 8%  |  Loss to fraud 1.1%

- Account Takeover: 1% (40)
- Card Not Present: 3% (63)
- Cheque Fraud: 1% (44)
- Employee Fraud: 2% (63)
- Corporate Identity Fraud: 2% (56)
- Computer Hacking: 8% (73)
- Computer Software: 2% (63)
- Fake Invoice Scams: 4% (81)
- Intellectual Property: 1% (41)
- Other: 2% (50)

Trust: Colleagues, Business Contacts & Peers, Accountant

() = Indices against survey average
Alison is a director at a small estate agent that has been in business for 17 years. She is aware of many fraud types but has never really experienced it. She is confident that her knowledge will stand her in good stead even though the company has taken few measures against fraud, except for having anti-virus software. She feels that internet crime poses a low threat to her business and that her IT company will protect her against fraud as much as possible.

“I haven’t done anything myself, but we do have anti-virus software”

“I feel that the risk from internet crime is very low at the moment”
Segment B
We’re worried but don’t have the time or knowledge to know what to do.

“I’m not very knowledgeable about fraud”

“We don’t have the resources or time to deal with it”

Segment B’s attitudes come from the fact that although they have little awareness of different types of frauds, they perceive themselves to be highly at risk. Their lack of knowledge, coupled with severe time pressure, makes them feel like they’re not in control.
UK enterprises: 903K (20%) | Total turnover: £248bn (17%) | Total fraud: £3.0bn (16%) | Fraud penetration: 26%

SME ATTRIBUTES

<table>
<thead>
<tr>
<th>SIZE</th>
<th>Percent %</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Micro - Single</td>
<td>21%</td>
<td>97</td>
</tr>
<tr>
<td>Micro</td>
<td>54%</td>
<td>115</td>
</tr>
<tr>
<td>Small</td>
<td>16%</td>
<td>63</td>
</tr>
<tr>
<td>Medium</td>
<td>9%</td>
<td>67</td>
</tr>
</tbody>
</table>

HEADCOUNT

<table>
<thead>
<tr>
<th>Change</th>
<th>Percent %</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decrease</td>
<td>12%</td>
<td>99</td>
</tr>
<tr>
<td>Same</td>
<td>72%</td>
<td>108</td>
</tr>
<tr>
<td>Increase</td>
<td>16%</td>
<td>85</td>
</tr>
</tbody>
</table>

TENURE

<table>
<thead>
<tr>
<th>Stage</th>
<th>Percent %</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Startup (&lt;3 yrs)</td>
<td>16%</td>
<td>100</td>
</tr>
<tr>
<td>Mid (3 to 10 yrs)</td>
<td>30%</td>
<td>100</td>
</tr>
<tr>
<td>Established (10+ yrs)</td>
<td>45%</td>
<td>100</td>
</tr>
</tbody>
</table>

TURNOVER

<table>
<thead>
<tr>
<th>Turnover</th>
<th>Percent %</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to £750,000</td>
<td>60%</td>
<td>103</td>
</tr>
<tr>
<td>£750,000 - £1.5m</td>
<td>10%</td>
<td>81</td>
</tr>
<tr>
<td>£1.5m - £6.5m</td>
<td>9%</td>
<td>69</td>
</tr>
<tr>
<td>£6.5m - £20m</td>
<td>2%</td>
<td>64</td>
</tr>
<tr>
<td>£20m - £40m</td>
<td>0%</td>
<td>-</td>
</tr>
<tr>
<td>£40m +</td>
<td>0%</td>
<td>-</td>
</tr>
</tbody>
</table>

TRADING

<table>
<thead>
<tr>
<th>Channel</th>
<th>Percent %</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Website</td>
<td>68%</td>
<td>82</td>
</tr>
<tr>
<td>Trade online</td>
<td>3%</td>
<td>82</td>
</tr>
<tr>
<td>Branches overseas</td>
<td>7%</td>
<td>77</td>
</tr>
</tbody>
</table>

SME FRAUD EXPERIENCE

EXPERIENCE

<table>
<thead>
<tr>
<th>Experience Type</th>
<th>Percent %</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud experience - last 12 months</td>
<td>26%</td>
<td>106</td>
</tr>
<tr>
<td>Cyber Fraud experience - last 12 months</td>
<td>11%</td>
<td>108</td>
</tr>
<tr>
<td>Loss to fraud % of turnover - last 12 months</td>
<td>1.2%</td>
<td>94</td>
</tr>
</tbody>
</table>

LOSS

<table>
<thead>
<tr>
<th>Loss Level</th>
<th>Percent %</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>We did not lose any</td>
<td>56%</td>
<td>107</td>
</tr>
<tr>
<td>Less than 1%</td>
<td>3%</td>
<td>84</td>
</tr>
<tr>
<td>1% - 3%</td>
<td>5%</td>
<td>71</td>
</tr>
<tr>
<td>3% - 5%</td>
<td>3%</td>
<td>91</td>
</tr>
<tr>
<td>More than 5%</td>
<td>3%</td>
<td>135</td>
</tr>
</tbody>
</table>

TYPE

<table>
<thead>
<tr>
<th>Fraud Type</th>
<th>Percent %</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Takeover</td>
<td>3%</td>
<td>125</td>
</tr>
<tr>
<td>Card Not Present</td>
<td>4%</td>
<td>78</td>
</tr>
<tr>
<td>Computer Software</td>
<td>4%</td>
<td>124</td>
</tr>
<tr>
<td>Computer hacking</td>
<td>12%</td>
<td>124</td>
</tr>
<tr>
<td>Cheque Fraud</td>
<td>3%</td>
<td>118</td>
</tr>
<tr>
<td>Fake Invoice Scams</td>
<td>3%</td>
<td>106</td>
</tr>
<tr>
<td>Intellectual Property</td>
<td>3%</td>
<td>106</td>
</tr>
<tr>
<td>Corporate Identity</td>
<td>3%</td>
<td>119</td>
</tr>
<tr>
<td>Employee Fraud</td>
<td>3%</td>
<td>93</td>
</tr>
<tr>
<td>Other types of Fraud</td>
<td>3%</td>
<td>99</td>
</tr>
</tbody>
</table>

Regional SME penetration

- Low
- Medium
- High

% = regional share of SMEs
Segment B

- **Key sectors**
  - F - Construction
  - D - Electricity, Gas, Steam And Air Conditioning Supply
  - A - Agriculture, Forestry And Fishing

- **Key attitudes**
  - Feel very at risk from fraud
  - Not knowledgeable about fraud and don’t know what to do about it

- **Key actions/inactions**
  - Do not have the time or resources to plan their security properly
  - Do not take all of the precautionary measures possible
  - Do not keep themselves up to date on fraudulent activity
  - React to things as they happen

- “We haven’t got the money or the capabilities to protect ourselves properly”
- “I use Streamline so I guess I am dependent on my credit card providers to make sure I am safe”
Segment B: Key attitudes

% Definitely and tend to agree

- We tend to react to things as they happen: 55 vs. 108
- Fraud happens but it is an acceptable cost of doing business: 11 vs. 68
- We are really concerned about fraud happening to the business: 33 vs. 112
- We have to make decisions quickly and sometimes there isn't time to be thoroughly diligent: 36 vs. 113
Segment B: Fraud experience

All Fraud 26% | Cyber fraud 11% | Loss to fraud 1.2%

Account Takeover: 3% (125)
Card Not Present: 4% (78)
Cheque Fraud: 3% (109)
Employee Fraud: 3% (83)
Corporate Identity Fraud: 3% (119)
Computer Hacking: 12% (118)
Computer Software: 4% (124)
Fake Invoice Scams: 5% (104)
Intellectual Property: 3% (105)
Other: 3% (98)

Trust: Police, Accountants

() = Indices against survey average
Mark runs a small catering company. He is very time poor, feels that he has set up business very quickly and that he hasn’t had time to attend to all parts of his company. He knows that fraud is something he needs to deal with but he doesn’t really know about all the different types of fraud, though he is especially worried about card fraud as he is planning to start taking card payments online. He would like to protect himself further but is not sure where to go to get more advice.

“I know there are many things I need to attend to and protecting against fraud is one of those. I just haven’t got the resource right now”
Segment C’s attitudes come from the fact that they have a low awareness of fraud and a low perceived risk. Fraud is not on their radar and it really is a case of out of sight out of mind.

"It’s not a threat to us"

"Fraud isn’t a common occurrence"

We don’t really need to think about fraud on a day to day basis
**Segment C**

**UK enterprises:** 959K (21%)  |  **Total turnover:** £239bn (16%)  |  **Total fraud:** £2.2bn (12%)  |  **Fraud penetration:** 18%

Annual fraud: £2.2bn (0.9% of turnover)

**MOSAIC Group profile**

**SME ATTRIBUTES**

<table>
<thead>
<tr>
<th>Size</th>
<th>0%</th>
<th>50%</th>
<th>100%</th>
<th>Percent %</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Micro - Single</td>
<td>32%</td>
<td>100%</td>
<td>100</td>
<td>144</td>
<td></td>
</tr>
<tr>
<td>Micro</td>
<td>47%</td>
<td>100</td>
<td>101</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small</td>
<td>15%</td>
<td>100</td>
<td>64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>6%</td>
<td>100</td>
<td>48</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**HEADCOUNT**

| Increase | 14% | 100 | 78 |
| Same     | 78% | 100 | 112 |
| Decrease | 10% | 100 | 71 |

**TENURE**

| Established (10+ yrs) | 45% | 100 |
| Mid (3 to 10 yrs)    | 40% | 102 |
| Start-up (<3 yrs)    | 16% | 97  |

**TURNOVER**

| £40 million + | 0% |
| £20 - £40 million | 0% |
| £8.5 - £20 million | 1% |
| £1.5 - £6.5 million | 9% |
| £750,000 - £1.5 million | 10% |
| Up to £750,000 | 68% |

**TRADING**

| External Website | 64% |
| Trade online    | 20% |
| Branches overseas | 8% |

**SME FRAUD EXPERIENCE**

<table>
<thead>
<tr>
<th>EXPERIENCE</th>
<th>0%</th>
<th>50%</th>
<th>100%</th>
<th>Percent %</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Fraud experience - last 12 months</td>
<td>19%</td>
<td>73</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fraud experience - last 12 months</td>
<td>8%</td>
<td>77</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss to fraud % of turnover - last 12 months</td>
<td>0.3%</td>
<td>72</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LOSS</th>
<th>0%</th>
<th>50%</th>
<th>100%</th>
<th>Percent %</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>We did not lose any..</td>
<td>56%</td>
<td>107</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Less than 1%</td>
<td>38%</td>
<td>111</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1%-3%</td>
<td>4%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3%-5%</td>
<td>0%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>More than 5%</td>
<td>1%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TYPE</th>
<th>0%</th>
<th>50%</th>
<th>100%</th>
<th>Percent %</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Takeover</td>
<td>1%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card Not Present</td>
<td>5%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer Software</td>
<td>1%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer hacking</td>
<td>8%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cheque Fraud</td>
<td>3%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fake Invoice Scams</td>
<td>2%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intellectual Property</td>
<td>1%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corporate Identity</td>
<td>1%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee Fraud</td>
<td>2%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other types of Fraud</td>
<td>2%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Regional SME penetration

- Low
- Medium
- High

% = regional share of SMEs

Links to segments: 35
Segment C

- **Key sectors**
  - T - Activities Of Households As Employers,
  - R - Arts, Entertainment And Recreation
  - Q - Human Health And Social Work Activities

- **Key attitudes**
  - Fraud is not on their radar
  - They tend to think that fraud will not happen to their company
  - They don’t feel that fraud is a common occurrence

- **Key actions/inactions**
  - They tend not to invest much in fraud defences, with neither external nor internal support
  - They don’t think about fraud as a serious threat
  - They don’t feel that they would change their business much if they suffered fraud

"When we migrate more of the business online we will be more worried, especially about payment processes"

"We don’t think we’re a particularly high risk organisation; we don’t see how people would invoice for more than they worked"
Segment C: Key attitudes

% Definitely and tend to agree

- Fraud is unlikely to happen to my company: 42% agree vs. 156% survey average
- We didn't lose any money so didn't do anything differently: 32% agree vs. 134% survey average
- We don't think about fraud: 27% agree vs. 173% survey average
- We know a lot about the methods fraudsters use: 22% agree vs. 70% survey average
Segment C: Fraud experience

All Fraud 18% | Cyber fraud 8% | Loss to fraud 0.9%

- Account Takeover: 1% (55)
- Card Not Present: 5% (85)
- Cheque Fraud: 3% (91)
- Employee Fraud: 2% (64)
- Corporate Identity Fraud: 1% (33)
- Computer Hacking: 6% (62)
- Computer Software: 1% (32)
- Fake Invoice Scams: 2% (44)
- Intellectual Property: 1% (32)
- Other: 2% (68)

Trust: Colleagues, Business Contacts & Peers, Friends & Family, Accountants

() = Indices against survey average
Segment C: Case study

Rebecca is the co-owner of a company that makes bespoke windows for private customers which has been in business for many years. She doesn’t really know much about fraud, as their company has never experienced it. She doesn’t really think about it very much either. The company shred documents but that’s about the only measure they take against fraud.

“We know most of our customers and go round to their houses so we trust them”

“I’ve heard of money laundering but I don’t know about any other types of fraud”
Segment D
“We have enough security in place”

“We have IT consultants who look after us”

We’ve been under siege but now we’ve taken necessary steps to protect ourselves

Segment D’s attitudes come from the fact that following previous experience of fraud, they have put prevention measures in place and now feel well protected. Despite this perception, they remain more at risk and lose more per business than any other segment.
### Segment D

**MOSAIC Group profile**

- **A** - Professional Services
- **B** - Professional Services
- **C** - Small Towns
- **D** - Rural Districts
- **E** - Service Industry
- **F** - Convenience
- **G** - New Businesses
- **H** - Councils
- **I** - Elderly
- **J** - Industrial Heritage
- **K** - High Street
- **L** - Liberal Opinion

**Annual fraud:** £2.4bn (1.5% of turnover)

**UK enterprises:** 138K (3%)  |  **Total turnover:** £153bn (10%)  |  **Total fraud:** £2.4bn (12%)  |  **Fraud penetration:** 30%

#### SME Attributes

<table>
<thead>
<tr>
<th>Size</th>
<th>0%</th>
<th>50%</th>
<th>100%</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Micro-Single</td>
<td>9%</td>
<td></td>
<td>50%</td>
<td>59</td>
</tr>
<tr>
<td>Micro</td>
<td>22%</td>
<td></td>
<td></td>
<td>68</td>
</tr>
<tr>
<td>Small</td>
<td>11%</td>
<td></td>
<td>50%</td>
<td>68</td>
</tr>
<tr>
<td>Medium</td>
<td>59%</td>
<td></td>
<td></td>
<td>448</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Headcount</th>
<th>0%</th>
<th>50%</th>
<th>100%</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decrease</td>
<td>17%</td>
<td></td>
<td></td>
<td>122</td>
</tr>
<tr>
<td>Same</td>
<td>58%</td>
<td></td>
<td></td>
<td>78</td>
</tr>
<tr>
<td>Increase</td>
<td>30%</td>
<td></td>
<td></td>
<td>167</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tenure</th>
<th>0%</th>
<th>50%</th>
<th>100%</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start-up (&lt;3 yrs)</td>
<td>10%</td>
<td></td>
<td>50%</td>
<td>65</td>
</tr>
<tr>
<td>Mid (3 to 10 yrs)</td>
<td>40%</td>
<td></td>
<td></td>
<td>102</td>
</tr>
<tr>
<td>Established (10+ yrs)</td>
<td>50%</td>
<td></td>
<td></td>
<td>110</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Turnover</th>
<th>0%</th>
<th>50%</th>
<th>100%</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to £750,000</td>
<td>37%</td>
<td></td>
<td></td>
<td>83</td>
</tr>
<tr>
<td>£750,000 - £1.5m</td>
<td>11%</td>
<td></td>
<td></td>
<td>62</td>
</tr>
<tr>
<td>£1.5 - £5.5m</td>
<td>28%</td>
<td></td>
<td></td>
<td>308</td>
</tr>
<tr>
<td>£5.5 - £20m</td>
<td>8%</td>
<td></td>
<td></td>
<td>296</td>
</tr>
<tr>
<td>£20 - £40m</td>
<td>9%</td>
<td></td>
<td></td>
<td>99</td>
</tr>
<tr>
<td>£40m +</td>
<td>7%</td>
<td></td>
<td></td>
<td>77</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trading</th>
<th>0%</th>
<th>50%</th>
<th>100%</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Website</td>
<td>99%</td>
<td></td>
<td></td>
<td>139</td>
</tr>
<tr>
<td>Trade online</td>
<td>93%</td>
<td></td>
<td></td>
<td>299</td>
</tr>
<tr>
<td>Branches overseas</td>
<td>20%</td>
<td></td>
<td></td>
<td>227</td>
</tr>
</tbody>
</table>

**SME Fraud Experience**

<table>
<thead>
<tr>
<th>Experience</th>
<th>0%</th>
<th>50%</th>
<th>100%</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>We didn't lose any</td>
<td>42%</td>
<td></td>
<td></td>
<td>81</td>
</tr>
<tr>
<td>Less than 1%</td>
<td>31%</td>
<td></td>
<td></td>
<td>134</td>
</tr>
<tr>
<td>1% - 3%</td>
<td>12%</td>
<td></td>
<td></td>
<td>154</td>
</tr>
<tr>
<td>3% - 5%</td>
<td>4%</td>
<td></td>
<td></td>
<td>116</td>
</tr>
<tr>
<td>More than 5%</td>
<td>2%</td>
<td></td>
<td></td>
<td>169</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Loss</th>
<th>0%</th>
<th>50%</th>
<th>100%</th>
<th>Index vs. survey avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Takeover</td>
<td>2%</td>
<td></td>
<td></td>
<td>121</td>
</tr>
<tr>
<td>Card Not Present</td>
<td>7%</td>
<td></td>
<td></td>
<td>134</td>
</tr>
<tr>
<td>Computer Software</td>
<td>5%</td>
<td></td>
<td></td>
<td>169</td>
</tr>
<tr>
<td>Computer Hacking</td>
<td>12%</td>
<td></td>
<td></td>
<td>156</td>
</tr>
<tr>
<td>Cheque Frauds</td>
<td>0%</td>
<td></td>
<td></td>
<td>95</td>
</tr>
<tr>
<td>Fake Invoice Scams</td>
<td>9%</td>
<td></td>
<td></td>
<td>119</td>
</tr>
<tr>
<td>Intellectual Property</td>
<td>3%</td>
<td></td>
<td></td>
<td>173</td>
</tr>
<tr>
<td>Corporate Identity</td>
<td>2%</td>
<td></td>
<td></td>
<td>173</td>
</tr>
<tr>
<td>Employee Fraud</td>
<td>7%</td>
<td></td>
<td></td>
<td>173</td>
</tr>
<tr>
<td>Other types of Fraud</td>
<td>7%</td>
<td></td>
<td></td>
<td>173</td>
</tr>
</tbody>
</table>

### Links to segments:

- 42
Segment D

- **Key sectors**
  - J - Information And Communication
  - K - Financial And Insurance Activities
  - L - Real Estate Activities

- **Key attitudes**
  - Think that the precautions they take will protect them, even though this segment is the most at risk from fraud
  - Believe they know a lot about fraud and can spot attempted frauds in progress

- **Key actions / inactions**
  - Proactive and don’t react to things as they happen
  - Often have IT consultants who look after their company online
  - Empowered and take personal responsibility for fraud

- **Statement**
  - “The only bad point about working online is the underlying investment needed to keep systems secure”

- **Statement**
  - “We have companies who regularly test our systems so they can’t be compromised”

- **Statement**
  - “We use Google Streetview to double check whether new suppliers actually exist”
Segment D: Key attitudes

% Definitely and tend to agree

Index vs. survey avg.

We don’t worry about fraud until it happens, then we’ll deal with it

My company has got enough security measures in place to protect us against any fraud

We know there is a lot of information out there to help businesses protect themselves...

We suffered fraud and took action to make sure it doesn't happen again
Segment D: Fraud experience

All Fraud 30%  |  Cyber fraud 12%  |  Loss to fraud 1.5%

Account Takeover: 2% (100)
Card Not Present: 7% (121)
Cheque Fraud: 0% (0)
Employee Fraud: 7% (173)
Corporate Identity Fraud: 2% (75)
Computer Hacking: 12% (116)
Computer Software: 5% (134)
Fake Invoice Scams: 8% (159)
Intellectual Property: 3% (119)
Other: 7% (225)

Trust: Colleagues, Business Contacts & Peers, Lawyer/Solicitor, IT Provider

() = Indices against survey average
Andy is the IT Director for a travel company with 200 employees. He is aware of many types of fraud and indeed they have been the victim of employee fraud in the past when an employee booked tickets for friends and family. They are now confident that the company is protected. They have many controls in place to protect against fraud, especially as this is demanded by their clients. All staff are now subject to background checks and are trained to look out for fraud. They even check employees’ home computers. The company have regular audits against fraud which are checked by an external auditor.

“We are not at risk from hardware attacks as we use three different companies that do penetrative tests monthly”

“We have lots of controls in place as our clients are law firms who demand it”
We’ve tried to protect ourselves and it didn’t work so now what do we do?

“We are very at risk”

“Whatever I do to protect myself, it’s never enough”

Segment E’s attitudes come from the fact that they feel past attempts to protect themselves from fraud haven’t worked. They continue to lose a high percentage of turnover to fraud and feel further efforts would not be fruitful.
UK enterprises: 362K (8%) | Total turnover: £199bn (13%) | Total fraud: £3.8bn (20%) | Fraud penetration: 37%

- **Annual fraud:** £3.8bn (1.9% of turnover)

**MOSAIC Group profile**

- **SIZE**
  - Micro - Single: 12%
  - Micro: 38%
  - Small: 20%
  - Medium: 22%

- **HEADCOUNT**
  - Decrease: 18%
  - Same: 68%
  - Increase: 28%

- **TENURE**
  - Startup (<3 yrs): 14%
  - Mid (3 to 10 yrs): 37%
  - Established (10+ yrs): 48%

- **TURNOVER**
  - Up to £759,999: 45%
  - £760,000 - £1.5 million: 17%
  - £1.5 - £6.5 million: 14%
  - £6.5 - £20 million: 4%
  - £20 - £40 million: 2%
  - £40 million+: 2%

- **TRADING**
  - External Website: 88%
  - Trade online: 64%
  - Branches overseas: 11%

**SME FRAUD EXPERIENCE**

- **EXPERIENCE**
  - Fraud experience - last 12 months: 37%
  - Cyber Fraud experience - last 12: 15%
  - Loss to fraud % of turnover - last 12: 1.9%

- **LOSS**
  - We did not lose any: 42%
  - Less than 1%: 33%
  - 1%-3%: 12%
  - 3%-5%: 10%
  - More than 5%: 3%

- **TYPE**
  - Account Takeover: 9%
  - Card Not Present: 9%
  - Computer Software: 9%
  - Computer hacking: 9%
  - Cheque Fraud: 9%
  - Fake Invoice Scams: 10%
  - Intellectual Property: 9%
  - Corporate Identity: 5%
  - Employee Fraud: 3%
  - Other types of Fraud: 6%

Links to segments: 49
Segment E

- Key sectors
  - G - Wholesale And Retail Trade, Repair Of Motor Vehicles
  - I - Accommodation And Food Service Activities
  - H - Transportation And Storage

- Key attitudes
  - Feel very at risk from fraud
  - Aware of common types of fraudulent activity
  - Whatever they do, they think it’s not enough to protect against everything

- Key actions/inactions
  - Have taken precautionary measures in the event of fraud
  - Have lost a high percentage of turnover to fraud
  - Kept up-to-date on common types of fraud
  - Feel that banks should be more proactive to help them

“I try to put things in place e.g. having an IT guy, but I don’t feel as if I’m one step behind or in front”

“Fraud is well dealt with on a personal level as the bank take care of it and there is no loss, but with a company we are treated differently”

“The banks should do more and be more proactive and be more responsible for transactions”
Segment E: Key attitudes

% Definitely and tend to agree

- Fraud is unlikely to happen to my company: 11 (42)
- We didn't lose any money so didn't do anything differently: 21 (88)
- We don't think anything we do would help protect us from fraud: 16 (147)
- We suffered fraud and took action to make sure it doesn't happen again: 52 (123)
Segment E: Fraud experience

All Fraud 37% | Cyber fraud 15% | Loss to fraud 1.9%

- Account Takeover: 6% (295)
- Card Not Present: 9% (165)
- Cheque Fraud: 6% (189)
- Employee Fraud: 8% (216)
- Corporate Identity Fraud: 5% (177)
- Computer Hacking: 16% (156)
- Computer Software: 6% (182)
- Fake Invoice Scams: 10% (197)
- Intellectual Property: 6% (212)
- Other: 6% (194)

Trust: Colleagues, Business Contacts & Peers, Friends & Family, Police

() = Indices against survey average
Segment E: Case study

Rupert is the Sales Director at a pharmaceutical company that has been around for 60 years. After losing money from fraud the company took specific action to protect themselves. However, the problems have continued including having their computer system hacked into and recently being the victim of a fake invoice scam. He feels frustrated and helpless and thinks the banks do not do enough to protect him against fraud.

“I think it’s the fault of the banks for not doing enough”

“There doesn’t seem to be any help or companies that we can go to for assistance with fraud”
Segment F’s attitudes come from the fact that even though they are aware and feel at risk from fraud, they are not motivated to act. They feel fraud is a part of every day life and it has a high penetration, but they are still unlikely to put proactive prevention measures in place.
UK enterprises: 372k (8%)  |  Total turnover: £175bn (12%)  |  Total fraud: £2.5bn (13%)  |  Fraud penetration: 42%

Annual fraud: £2.5bn (1.4% of turnover)

MOSAIC Group profile

Size
- Micro - Single: 11%
- Micro: 45%
- Small: 22%
- Medium: 22%

Headcount
- Decrease: 19%
- Same: 58%
- Increase: 22%

Tenure
- Start-up (<3 yrs): 18%
- Mid (3 to 10 yrs): 30%
- Established (10+ yrs): 42%

Turnover
- Up to £759,999: 47%
- £760,000 - £1.5m: 17%
- £1.5 - £5.5m: 14%
- £5.5 - £20m: 3%
- £20 - £40m: 2%
- £40m +: 2%

Trading
- External Website: 98%
- Trade online: 96%
- Branches overseas: 11%

Links to segments: 56

Percent %
Index vs. survey avg.

EXPERIENCE
- Fraud experience - last 12 months: 42%
- Cyber Fraud experience - last 12 months: 17%
- Loss to fraud % of turnover - last 12 months: 1.4%

LOSS
- We did not lose any: 47%
- Less than 1%: 33%
- 1%-3%: 15%
- 3%-5%: 5%
- More than 5%: 3%

TYPE
- Account Takeover: 3%
- Card Not Present: 12%
- Computer Software: 7%
- Computer hacking: 17%
- Cheque Fraud: 9%
- Fake Invoice Scams: 6%
- Intellectual Property: 6%
- Corporate Identity: 3%
- Employee Fraud: 6%
- Other types of Fraud: 6%

Regional SME penetration

% = regional share of SMEs
Segment F

- **Key sectors**
  - G - Wholesale And Retail Trade, Repair Of Motor Vehicles
  - H - Transportation And Storage
  - I - Accommodation And Food Service Activities

- **Key attitudes**
  - They don’t feel that fraud is a big deal and think they are no more at risk than anyone else
  - They feel being at risk is just an inevitable part of doing business today
  - They are not really aware of all the different types of fraud

- **Key actions/inactions**
  - They aren’t as organised and careful in their working practices as they could be
  - They tend to react to things as they happen
  - They assume their IT companies will take care of fraud for them

“We are at risk no more or less than anyone else”

“We shred our documents, not really anything else to be honest. I put my faith in Barclays and Paypal to do it for us.”

“We have someone who does our web and he assures me that we are okay. I don’t worry about it until the day it happens”
Segment F: Key attitudes

% Definitely and tend to agree

We carry out a lot of business online and therefore don't know who we are dealing with

Fraudsters target our company regularly but we pick up on it before it can happen

Fraud is not a big deal for SMEs

If fraud happens again we would deal with it in the same way

Index vs. survey avg.

36  200
20  180
11  152
21  178
Segment F: Fraud experience

All Fraud 42% | Cyber fraud 17% | Loss to fraud 1.4%

- Account Takeover: 3% (148)
- Card Not Present: 12% (223)
- Cheque Fraud: 8% (275)
- Employee Fraud: 6% (165)
- Corporate Identity Fraud: 8% (285)
- Computer Hacking: 17% (168)
- Computer Software: 7% (208)
- Fake Invoice Scams: 6% (127)
- Intellectual Property: 8% (303)
- Other: 6% (169)

Trust: Colleagues, Business Contacts & Peers, Lawyer/Solicitor, Accountants

() = Indices against survey average
John is a Sales Director at an exhibition and displays company that has been in business for 20 years. He has experienced fraud in the past, but it wasn’t very serious as the company didn’t lose any money. He feels fraud is a typical part of being in business today - things are always risky, whatever you do. He employs someone to do his IT and advise him on how to protect his business but is usually content to let things take their natural course.

“We do have a firewall but that is it”

“Not aware of supplier fraud, don’t really know much about phishing e-mails either”
Communications strategy
Four key communication themes

**Awareness**
Create awareness for those who don’t even have fraud on their radar or understand the different types.

**Create reassurance and give control**
This is for segments that, while worried, don’t feel they know where to go for help.

**Challenging complacency**
This is for segments that may have a false sense of security in thinking they have fraud under control.

**Creating a sense of urgency to act**
This is for segments that think fraud may hit them but that it won’t really damage their business.
# Communications matrix

<table>
<thead>
<tr>
<th></th>
<th>Awareness</th>
<th>Create reassurance and give control</th>
<th>Challenge complacency</th>
<th>Create urgency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segment A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Segment B</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Segment C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Segment D</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Segment E</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Segment F</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Excellent fit**
- **Good fit**
## Summary

<table>
<thead>
<tr>
<th>Segment</th>
<th>Key segment dimensions</th>
<th>Attitude summary</th>
<th>Key issue</th>
<th>Comms. themes</th>
</tr>
</thead>
</table>
| Segment A | High Awareness  
Low Perceived Risk  
At Risk | We’re knowledgeable about fraud  
and think we can spot it so it won’t  
happen to us | Knowledge alone won’t protect them | Challenging complacency |
| Segment B | Low Awareness  
High Perceived Risk  
At Risk | We’re worried about fraud but don’t  
have the time or knowledge to know  
what to do | Lack time and confidence | Take Control |
| Segment C | Low Awareness  
Low Perceived Risk  
At Risk | We don’t really need to think about  
fraud on a day to day basis | Fraud is not on their radar | Raise Awareness |
| Segment D | High Awareness  
Low Perceived Risk  
Extremely at Risk | We’ve been under siege from  
fraudsters but now we’ve taken  
necessary steps to protect ourselves | Low perceived risk is misplaced  
as they are still highly at risk | Challenging complacency |
| Segment E | High Awareness  
High Perceived Risk  
Highly at Risk | We’ve tried to protect ourselves and it  
didn’t work so now what do we do? | Over coming sense of victim  
mentality | Take Control |
| Segment F | Low Awareness  
High Perceived Risk  
Highly at Risk | Fraud’s just a fact of life that we will  
deal with at the time | They are on borrowed time | Create a sense of urgency to act |
Segment comparisons
Segment comparisons
Key variables
4.5 Million UK SMEs by segment

Counts of enterprises by segment

Thousands

- Segment A: 1,801
- Segment B: 903
- Segment C: 959
- Segment D: 138
- Segment E: 362
- Segment F: 372
Segment D is made up of larger SMEs

Size of enterprise by segment

- Segment A: 76% Micro, 18% Small, 6% Medium
- Segment B: 75% Micro, 16% Small, 9% Medium
- Segment C: 79% Micro, 15% Small, 6% Medium
- Segment D: 58% Micro, 31% Small, 11% Medium
- Segment E: 50% Micro, 28% Small, 22% Medium
- Segment F: 56% Micro, 22% Small, 22% Medium
SME turnover by segment

**Percentage of SMEs**

- **Segment A**: 11%, 9%
- **Segment B**: 10%, 9%
- **Segment C**: 10%, 9%
- **Segment D**: 23%, 9%
- **Segment E**: 17%, 14%
- **Segment F**: 17%, 14%

**Index vs. SME average**

- **Segment A**: Index 48, 83, 110
- **Segment B**: Index 81, 88, 103
- **Segment C**: Index 81, 82, 114
- **Segment D**: Index 63, 90, 209
- **Segment E**: Index 77, 144, 258
- **Segment F**: Index 80, 140, 230
Segments E and F have experienced fraud the most in the last 12 months

Percentage who have experienced fraud in the last 12 months

- Segment A: All fraud 19%, Cyber fraud 8%
- Segment B: All fraud 26%, Cyber fraud 11%
- Segment C: All fraud 18%, Cyber fraud 8%
- Segment D: All fraud 30%, Cyber fraud 12%
- Segment E: All fraud 37%, Cyber fraud 15%
- Segment F: All fraud 42%, Cyber fraud 17%
With Segment E losing the highest proportion of their turnover

Percentage of turnover lost to fraud by segment

- Segment A: 1.1%
- Segment B: 1.2%
- Segment C: 0.9%
- Segment D: 1.5%
- Segment E: 1.9%
- Segment F: 1.4%
When they are hit, Segment D experiences the highest absolute loss

**Average 12 month loss (per SME experiencing fraud)**

\[
\text{12 month loss} = \text{Turnover} \times \% \text{ turnover lost to fraud} \\
\text{(mid-points of turnover and fraud % lost bands used)}
\]

\[
\text{Base} = 1225 \text{ (where respondents reported both turnover and % loss to fraud)}
\]

<table>
<thead>
<tr>
<th>Segment</th>
<th>Average Loss (£)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segment A</td>
<td>£9,828</td>
</tr>
<tr>
<td>Segment B</td>
<td>£13,239</td>
</tr>
<tr>
<td>Segment C</td>
<td>£7,143</td>
</tr>
<tr>
<td>Segment D</td>
<td>£92,120</td>
</tr>
<tr>
<td>Segment E</td>
<td>£39,099</td>
</tr>
<tr>
<td>Segment F</td>
<td>£47,518</td>
</tr>
</tbody>
</table>
When they are hit, Segment D experiences the highest absolute loss

**Average 12 month loss (per SME experiencing fraud and losing money)**

12 month loss = Turnover * % turnover lost to fraud
(mid-points of turnover and fraud % lost bands used)

Base = 594 (where respondents reported both turnover and % loss to fraud was greater than 0)

- **Segment A**: £12,453
- **Segment B**: £14,716
- **Segment C**: £8,490
- **Segment D**: £116,896
- **Segment E**: £58,304
- **Segment F**: £55,697
UK market size: segment share of enterprises, turnover and fraud loss

Segment share %

- Segment A: All SME 40%, Turnover 32%, Loss to fraud 27%
- Segment B: All SME 20%, Turnover 17%, Loss to fraud 16%
- Segment C: All SME 21%, Turnover 16%, Loss to fraud 12%
- Segment D: All SME 3%, Turnover 10%, Loss to fraud 12%
- Segment E: All SME 8%, Turnover 13%, Loss to fraud 12%
- Segment F: All SME 8%, Turnover 12%, Loss to fraud 13%

SME count of enterprises = 4.5 Million (BIS)
Turnover total £ = £1.5 Trillion (BIS)
Estimated loss £ = £18.9 Billion (NFA)
Segment comparisons
Geo-demographics
High indexing MOSAIC groups are very similar across segments.
Top 5 Mosaic groups

**Alpha Territory**
- Highest indexing age band 56 - 60
- Successful
- Rewarding careers
- Substantial wealth
- Influential
- Wealthy foreign nationals
- Fashionable areas of London
- Specialist advice
- Professional
- Well educated

**Professional Rewards**
- Highest indexing age band 61 - 65
- Suburban
- Small businesses
- Senior positions
- Significant equity
- Married with children
- Comfortable
- Good education
- Theatre / arts
- Car ownership

**Rural Solitude**
- Highest indexing age band 61 - 65
- Country pursuits
- High motor costs
- Large buildings
- Married
- Small businesses
- Farmers with Isolated farmhouses
- Community spirit
- Small villages
- Mature

**Careers and Kids**
- Highest indexing age band 31 - 35
- Families with Young Children
- Good incomes
- Comfortable homes
- Home life balance
- Ethical products
- Consumer credit
- Reliant on cars
- Internet and telephone banking
- New buildings

**Liberal Opinions**
- Highest indexing age band 18 - 25
- Young singles
- Students
- Degree level education
- Creative jobs
- Vibrancy / Diversity
- Ethical products
- Internet searches
- Theatre and arts
- Cinema
High indexing FSS groups are also similar across segments
Top FSS groups

Accumulated Wealth
- Affluent families
- Highest income
- High status careers
- Expensive homes
- Wide range of investments
- Stocks and shares
- Equity ISAs
- Property as investment
- Good pension savings
- High insurance spend
- Sophisticated knowledge
- High use of internet
- Move money to find best returns

Index: 500

Growing Rewards
- Families in 30s and early 40s
- Growing children
- Two professional salaries
- High mortgage commitments
- Well educated
- High status jobs
- Quality detached homes
- Good start to savings
- High potential to increase investments
- Children’s savings accounts
- High spend on insurance
- Life insurance
- Critical illness cover
- High use of internet

Index: 146

Consolidating Assets
- Families in 40s and early 50s
- Good start to investments
- Adding to savings regularly
- Growing equity in home
- Some support older children
- Above average salaries
- Good education
- Detached or semi family homes
- Cash ISAs
- Premium bonds
- Pension saving
- Regular internet users

Index: 260

Established Reserves
- Aged in late 50s or early 60s
- Good salaries
- Some retired early or working part time
- Reducing financial commitments
- Respectable savings
- Some adult children to support
- Comfortable homes
- Own outright
- Savings for retirement
- Cash ISAs
- Premium bonds
- Good pension provision

Index: 146
Segments share very similar TrueTouch profiles
Top TrueTouch types

**Information @ Speed**
- Male 36-55
- Heavy internet users
- Latest technology
- Use web as information source
- Use remote ways to assess finance
- Magazines/telecommunication as source of information
- Radio/TV for business and general news
- Teletext and interactive TV for share prices
- Heavy use of mobiles for business productivity

**Practical Surfers**
- Male 36-55
- Use internet for practical purposes
- Confident in their own assessment of information
- Confident in financial matters
- No concerns with identity theft or security
- Heavy radio listeners
- Interactive TV for sports and business
- Influenced by financial TV ads and direct mail

**Virtual Experimenter**
- Married aged 55-65
- Learning to utilise modern technology
- Comfortable lifestyle
- High management positions
- Heavy readers of broadsheet newspapers
- No concern of identity theft or security
- Use telephone and internet for sales activity
- Heavy post users
- Adamant decision style

**Intellectual Digerati**
- Male or Female
- Single aged 26-45
- Rely on internet and mobiles
- Always use internet as first source of information
- Latest technology
- High mobile phone bills
- Mobile banking
- Listen to expert advice
- Light TV viewers
- Communication is always via technology
# Top 3 types by segments

<table>
<thead>
<tr>
<th>Segment</th>
<th>Mosaic</th>
<th>FSS</th>
<th>TrueTouch</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Segment A</strong></td>
<td>B07 Distinctive Success A03 Business Class A02 Voices of Authority</td>
<td>F19 Self-made Success F18 Asset Accruers F20 Golden Outlook</td>
<td>F21 Virtual Experimenters A01 Information@speed A04 Intellectual Digerati</td>
</tr>
<tr>
<td><strong>Segment B</strong></td>
<td>A03 Business Class B07 Distinctive Success A04 Serious Money</td>
<td>F19 Self-made Success F18 Asset Accruers G21 Sound Positions</td>
<td>F21 Virtual Experimenters A01 Information@speed A02 Practical Surfers</td>
</tr>
<tr>
<td><strong>Segment C</strong></td>
<td>A03 Business Class A02 Voices of Authority A04 Serious Money</td>
<td>F19 Self-made Success F20 Golden Outlook F18 Asset Accruers</td>
<td>A01 Information@speed F21 Virtual Experimenters A04 Intellectual Digerati</td>
</tr>
<tr>
<td><strong>Segment D</strong></td>
<td>A01 Global Power Brokers B07 Distinctive Success O63 Urban Cool</td>
<td>F17 Fast-track Fortunes F19 Self-made Success G21 Sound Positions</td>
<td>A01 Information@speed F21 Virtual Experimenters A02 Practical Surfers</td>
</tr>
<tr>
<td><strong>Segment E</strong></td>
<td>O61 Convivial Homeowners O64 Bright Young Things A04 Serious Money</td>
<td>F18 Asset Accruers F20 Golden Outlook G22 Single Accumulators</td>
<td>F21 Virtual Experimenters A04 Intellectual Digerati A01 Information@speed</td>
</tr>
<tr>
<td><strong>Segment F</strong></td>
<td>A03 Business Class A02 Voices of Authority O63 Urban Cool</td>
<td>A03 Early Settlers F17 Fast-track Fortunes F19 Self-made Success</td>
<td>F21 Virtual Experimenters A01 Information@speed A02 Practical Surfers</td>
</tr>
</tbody>
</table>
Mapping to the consumer segments
Consumer Segment 4 matches all SME segments (based on age, gender and geodemographics)

Segment 4: Risk takers seeking financial gain

<table>
<thead>
<tr>
<th>SME Business Segment</th>
<th>Consumer Segments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>A</td>
<td>0.93</td>
</tr>
<tr>
<td>B</td>
<td>0.93</td>
</tr>
<tr>
<td>C</td>
<td>0.86</td>
</tr>
<tr>
<td>D</td>
<td>0.77</td>
</tr>
<tr>
<td>E</td>
<td>0.88</td>
</tr>
<tr>
<td>F</td>
<td>0.80</td>
</tr>
</tbody>
</table>

-1 = Negative correlation, +1 = Highest positive correlation

- Spearman’s Rank correlation was used to find the differences between the two segment groups. The closer the figure to 1, the closer the relationship.
Consumer Segment 4: Risk takers seeking financial gain - summary

Segment 4 (21% of UK Adults)
Risk takers seeking financial gain
Affluent, opportunity seeking professional males – “because of greed I became a victim”

Who we are:
- Age 35-55
- Singles & Families
- Affluent/comfortably off
- Detached
- Online banking & money management
- Financially Aware

Experience, attitudes and awareness of fraud:
- ID Fraud
- Phishing emails
- Bank Card Fraud
- Property Investment Scams
- Foreign money making investments
- Confident & Assured
- Risk seekers & financially impulsive

Key Requirements:
This is a confident and assured segment that profess financial competence and maturity – communications should demonstrate that risky behaviours and acting on impulse heighten the likelihood of material loss and are not the actions of competent professionals.

Total fraud loss: £3.35bn
- £2.70bn
- £1.17bn
- £0.16bn

Communication Preferences
- Web
- Email
- Newspapers

Risk Avoidance Behaviours
- High Risk/Careless Behaviours
- Low Risk/Cautious Behaviours

Overall Risk
- High Risk/Careless Susceptibility
- Low Risk/High Susceptibility
Consumer Segment 4: Risk takers seeking financial gain - profiles

Segment 4 (21% of UK Adults)
Risk takers seeking financial gain
Affluent, opportunity-seeking professional males at risk - "because of greed"
## Consumer Segment 4:
Match to SME segments based on attitudes

<table>
<thead>
<tr>
<th>Consumer questions</th>
<th>SME questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud is unlikely to happen to me</td>
<td>Fraud is unlikely to happen to my company</td>
</tr>
<tr>
<td>Fraud is becoming more common</td>
<td>Fraud is becoming more common</td>
</tr>
<tr>
<td>I would know if I was exposed to fraud</td>
<td>We would be able to spot fraud</td>
</tr>
<tr>
<td>I feel I know a lot about fraud and the methods people use</td>
<td>We know a lot about the methods fraudsters use</td>
</tr>
<tr>
<td>You have to be a bit stupid/naive to fall for a fraud</td>
<td>We’d have to be stupid/naïve to fall for a fraud</td>
</tr>
</tbody>
</table>
Consumer segment 4: Match to SME segments based on attitudes

Risk takers seeking financial gain

Stronger match

Segment E
Segment F
Segment D
Segment A
Segment B
Segment C

Weaker match
Appendix
## Key segment dimension summary

<table>
<thead>
<tr>
<th></th>
<th>Experience of fraud</th>
<th>Actual risk of fraud</th>
<th>Perceived risk of fraud</th>
<th>Awareness of fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segment A</td>
<td>Low</td>
<td>At Risk</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Segment B</td>
<td>Medium</td>
<td>At Risk</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Segment C</td>
<td>Low</td>
<td>At Risk</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Segment D</td>
<td>Medium</td>
<td>Extreme</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Segment E</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Segment F</td>
<td>High</td>
<td>Extreme</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>

**Notes:**
- **Fraud experience** = Penetration of businesses having experience fraud in the last 12 months
- **Actual risk** = Modelled risk based on business attributes – see Building the Segments
- **Perceived risk** = whether the businesses thought they were at risk
- **Awareness** = An aggregate score of how aware businesses were of 9 different types of fraud – see fraud definitions in appendix
The segmentation process

- **Stage 1 - Qualitative stage**
  - Telephone interviews to establish key attitudes to fraud
  - 26 SME business owners / key decision makers interviewed
  - Across a range of businesses by sectors, size and region.

- **Stage 2 - Quantitative marketing survey**
  - To test and establish hypotheses from stage 1
  - 2,400 respondents across a range of businesses by sectors, size and region.

- **Stage 3 - Segmentation and modelling**
  - Establish key segment dimensions using the quantitative survey data
  - Modelling actual risk using business attributes from the survey data
  - Cluster analysis to group like-minded SMEs on key dimensions
The segmentation process

- Stage 4 – Cross-referencing the SME fraud segments to the consumer fraud segments
  - Using geo-demographic profiles, age, gender and attitudes.

- Stage 5 – Fusion to Touchpoints 4 media planning tool
  - Segment individuals fused to Touchpoints individuals.
Additional data sources

- Fraud estimates
  - Annual Fraud Indicator – March 2012 -

- SME counts
  - Department for Business Innovation and Skills – October 2011
    http://www.bis.gov.uk/analysis/statistics/business-population-estimates

- Market statistics:
  - SME enterprises: 4.5 Million (BIS)
  - SME 12-month fraud - £18.9 Billion (NFA)
SME definitions

SME size

- **Micro** = Single owner businesses and up to 9 employees
- **Small** = 10 to 49 employees
- **Medium** = 50 to 249 employees
Fraud type definitions

- **Account takeover** - when a fraudster gains control of an account and then makes unauthorised transactions.

- **Card not present fraud** - fraudulent use of credit/debit card details to purchase products or services in a non face-to-face setting.

- **Cheque fraud** – where a fraudster pays for goods or services using a stolen or counterfeit cheque.

- **Computer software service fraud** - where fraudsters impersonate legitimate software companies to get credit card information and passwords.

- **Computer hacking** – remotely breaking into computers/computer networks and accessing sensitive information (fraud occurs when money is lost as a result).

- **Employee fraud** - when fraud is committed by someone against the company they are working for. Examples include: diverting payments, ‘fiddling’ expenses and exploiting company assets and information (including customer data).

- **Fake invoice scams** - when fraudsters send fake invoices and requests for payment for goods and services that haven't been ordered or received.

- **Intellectual property fraud and theft** – when fake goods are passed off as originals or plans, drawings or details of industrial processes are stolen.

- **Corporate identity fraud** – when company details are stolen used to commit fraud, such as opening bank accounts or ordering goods in your company’s name.