Identifying Online Fraud through Mouse Movement Behavior

Markus Weinmann
University of Liechtenstein

Joseph S. Valacich
University of Arizona

Christoph Schneider
City University of Hong Kong

Jeffrey L. Jenkins
Brigham Young University

Martin Hibbeln
University of Duisburg-Essen

September 26, 2017

***** WORKING PAPER – PLEASE DON'T DISTRIBUTE *****

Abstract

Organizations are increasingly interacting with customers through online channels. While providing numerous benefits to both organizations and customers, the move to online interaction has fueled an associated increase in online fraud. In this paper, we report the results of two observational studies, using vastly different tasks, where online participants could freely decide to commit fraud to financially benefit themselves. In Study 1, 19% of the interactions were fraudulent; in Study 2, 20% of the interactions were fraudulent. In both studies, we captured mouse movement data while participants completed their online task. As predicted, when committing fraud, participants in both studies moved their mouse significantly slower and with greater deviations than non-fraudulent interactions. Additionally, we used mouse movements to infer which participant interactions were fraudulent. In Study 1, the prediction accuracy was 82%; in Study 2, the prediction accuracy was 93%. The results provide evidence that monitoring mouse movements can aid in identifying online fraud.

Keywords: mouse movements, online fraud, human-computer interaction, cognitive dissonance, cognitive conflict, cognitive load, observational study

Identifying Online Fraud through Mouse Movement Behavior

Introduction

Gartner predicts that by 2020 nearly all modern organizations will compete primarily through online channels (Pettey 2015). As the online revolution continues to accelerate, countless organizations require people to complete online forms to submit applications, file claims, request services, or report events. Whereas most people submit legitimate and genuine information, there is also a large and growing number of people who knowingly provide fraudulent information (Meola 2016; Vuitton 2017). While often considered a "victimless crime" (e.g., Morley et al. 2006), fraud causes tremendous costs for organizations, governments, and ultimately for society, as the upright citizen covers the cost of fraud.

Conducting business online has been a catalyst for increased fraudulent behavior (Sorrell 2017). There are many types of online fraud, some of which are related to account creation (i.e., identity theft), account takeover (e.g., phishing attacks), and transactions (e.g., disputing receipt of a delivered product). Such general fraud categories exist in one way or another across many governmental and organizational sectors, including e-commerce, banking, insurance, and healthcare, to name a few. For example, in the insurance industry, fraud can range from providing inaccurate information on insurance applications to submitting exaggerated claims (sometimes referred to as "padding"), or submitting claims for unnecessary repairs or procedures. As these types of fraud may not only be committed by the insurance holders or applicants, but also third parties or claims professionals, online fraud can have tremendous financial consequences. For instance, in the United States alone, insurance claim fraud is the second largest white collar crime after tax evasion (Dean 2004), amounting to yearly damages of around US$80 billion (Coalition Against Insurance Fraud 2017; Coolidge 2006; Smith 2000).

Like in many industries, insurance claim auditors struggle to identify fraud, as it is infeasible to carefully underwrite and review all submitted applications and claims. While most of the applications and claims are likely to be genuine, some are fraudulent—ranging from slight inadvertent misrepresentations to those filed with fully fraudulent intent. For example, 10 percent of Americans surveyed in 2017 admitted to misrepresenting information on auto insurance applications (e.g., reported lower annual mileage, misstated how a car would be used, etc.) in order to get a better rate (Glover 2017). Often, auditors identify and review only those applications and claims viewed to be most egregious. Thus, identifying all fraudulent applications and claims is a "needle in the haystack problem," as it is impractical and very costly, both in time and money, to thoroughly vet all submitted information. Also, when auditors delay legitimate applications and claims due to additional scrutiny, they risk lowering the customer experience and are much more likely to dissatisfy and potentially lose honest customers (Kulbytė 2017). Therefore, improving methods for more quickly and reliably identifying potential fraudulent information can provide benefits to honest consumers, service providers, and society as a whole.

Studies suggest that mouse movements can reveal hidden psychological states that traditional measures cannot capture (Freeman et al. 2011). For example, mouse movements can be influenced by emotional arousal and valence (e.g., Grimes et al. 2013), cognitive conflict (e.g,. Dale et al. 2007), and increased cognitive processing (Freeman and Ambady 2011). Consequently, Valacich et al. (2013) suggested monitoring people's mouse movements to detect behavioral patterns that may be indicative of fraudulent responses. Relatedly, recent research has shown that mouse movements can be used to identify people who conceal information in a structured question protocol after engaging in a sanctioned (i.e., mock) crime (Anonymous,

under review). However, there are many significant weaknesses related to the use of sanctioned deception—e.g., low motivation of participants, lack of ecological validity, low stakes, and so on (Buckley 2012; Sip et al. 2008)—as well as the time lag between the mock task and administering the structured interviews (Ben-Shakhar 2012). While research has suggested that mouse movements may be influenced when engaging in a deceptive act (e.g., Valacich et al. 2013), limited research has theoretically developed and empirically validated hypotheses on *how* deception influences mouse movements. Here, we extend the prior work by collecting movement data when participants freely choose to engage in a fraudulent act. Thus, this research overcomes the weakness of sanctioning and time delays between the fraudulent act and movement collection.

Drawing on theory from psychology and neuroscience, we theoretically explain and empirically validate how one type of deception – online fraud – influences people's hand movements, and thereby mouse-cursor movements (hereafter, simply "mouse movements"). In doing so, we answer our first research question: *How does online fraud meaningfully influence mouse movements?* As we are focused on how specific types of mouse movements can be used to infer online fraud, we answer the second research question: *Can online fraud be inferred from mouse movements?* To answer these research questions, we report two studies. In the first, we used an established visual-perception task that incentivized participants to commit fraud. In particular, participants responded to a binary question while we measured their mouse movements. In the second, we focused on online insurance claims. Here, we asked participants to complete a sequence of online damage-reporting forms, and recorded and analyzed their mouse movements. The results of both studies show that 1) fraud leads to predictable changes in mouse-movement behavior–i.e., increasing deviations and decreasing speed–and 2) committing online

fraud can be inferred from such changes in mouse behavior. This provides a foundation for improving the design of online forms to better identify those providing fraudulent information.

Background

Online fraud is widespread, causing billions of dollars in losses for businesses and governments. Such losses result in increased costs for consumers and fewer services to citizens. Unfortunately, people commit fraud in various ways—for example, dishonest insurance policyholders can file claims that never occurred or exaggerate actual losses to reclaim their deductible (many insurance fraudsters perceive deductibles as being unfair) (Clarke 1990)—so no single detection method will detect all types of fraud. While insurance companies have historically relied on auditing to mitigate the effects of fraud, they—and other industries—are increasingly using triangulation, e.g., by augmenting auditing procedures with information obtained from fraud-detection systems, using various fraud indicators and classification techniques (e.g., Dionne et al. 2009; Schiller 2006).

Given the prevalence of online fraud, organizations are exploring a variety of new and novel ways to efficiently and effectively identify potential fraud. For example, organizations are increasingly using a variety of techniques, ranging from statistical (e.g., clustering, anomaly detection, etc.) to artificial intelligence-based (e.g., data mining, machine learning, etc.) approaches to uncover potential fraud (Carneiro et al. 2017; Lopez-Rojas and Axelsson 2016; Save et al. 2017). Identifying and validating new and emerging fraud-detection techniques are crucial for business and society, as a higher detection accuracy lowers the costs of ex-post monitoring. Because thorough monitoring is costly, auditors typically investigate only those applications and claims that appear to be most egregious but many “small” misrepresentations simply slip through the cracks, collectively equating to billions of dollars (Hunter 2015). Thus,

there is clearly a need to improve fraud-detection systems by exploiting additional low-cost signals of potential fraud.

To this end, we propose and test a low-cost and highly scalable method for detecting possible fraud when people provide online information by monitoring users' mouse movements. Mouse movements have been found to give insight into many cognitive and emotional processes (see Freeman et al. 2011 for a brief literature review), some of which can result from deception, including decision conflict (McKinstry et al. 2008; Palmer et al. 2013), cognitive competition (Dale et al. 2007; Freeman and Ambady 2009; Freeman and Ambady 2011; Freeman et al. 2008), emotional reactions (Grimes et al. 2013; Maehr 2008; Rodrigues et al. 2013; Zimmermann et al. 2006; Zimmermann et al. 2003), and increased cognitive processing (Freeman and Ambady 2011). More specifically, in some studies, mouse movements have been proposed to indicate deception directly. For example, Valacich et al. (2013) created (but not tested) propositions that explain how mouse movements may indicate deception in concealed information tests.

Our research contributes to theory and practice by explaining and empirically validating how mouse movements are influenced by intentional fraud when completing online forms.

Hypotheses

To develop hypotheses that explain how fraud correlates with mouse movements, we build on two axioms of deception—cognitive dissonance / conflict and cognitive load.

First, when being deceptive, people experience cognitive or moral conflict (Buller and Burgoon 1996; Nunez et al. 2005). For example, due to guilt or fear of being caught, deceptive people are more likely to experience hesitations as they reconsider their planned and current actions. Likewise, such people are more likely to experience increased cognitive dissonance /

conflict by questioning and reconsidering their planned fraudulent actions (Derrick et al. 2013; Nunez et al. 2005).

Such competing cognitions can influence one's movements, as explained by the response activation model (RAM) (Welsh and Elliott 2004). Namely, the RAM posits that one's hand movements respond to all cognitions (i.e., thoughts) that have even a small potential to result in movement, so-called *actionable potential* (Welsh and Elliott 2004). As such, when people knowingly provide misleading information when completing an online form, they are also more likely to deal with competing cognitions like double checking, reconsidering, hesitating, or questioning actions. For example, when moving the mouse to commit fraud in an online form, one may have a thought to stop the action due to fear of being caught; likewise, one may have a thought to respond differently to result in a more believable fraud (e.g., moving the mouse to select a different option). Such thoughts have actionable potential (e.g., to stop or to move differently)—even if the actions are not executed—resulting in increased deviations (e.g., direction and speed changes), that are less likely to occur if being non-fraudulent.

The RAM explains the relationship between thoughts and mouse movements: When a thought with actionable potential enters the mind (i.e., is in working memory), the mind automatically and subconsciously programs a movement response to fulfil that cognition's intention (Welsh and Elliott 2004). This includes transmitting nerve pulses to the muscles to move the hand and realize the intention (i.e., stop or move) (e.g., Georgopoulos 1990; Song and Nakayama 2008). These nerve impulses, in turn, ultimately result in hand movements toward the stimulus. If a person had accordant cognitions, their mouse trajectory would roughly follow a straight line to the movement's target (e.g., to the intended input field on the online form). Deviations from that straight line can result from competing cognitions due to being

fraudulent—i.e., the mind programs movement responses toward other stimuli with actionable potential. Those deviations can also be captured by characteristics of the mouse movements. In summary, we hypothesize:

H1: When providing fraudulent responses in an online form, people will exhibit greater mouse deviation.

Second, deception is a complex cognitive process that increases cognitive load, another axiom of deception (Carrión et al. 2010). If people deceive they not only have to generate false information but typically also attempt to minimize evidence of deception (Derrick et al. 2011). Handling both requires people to behave strategically—i.e., manage information to appear truthful—which increases cognitive load, thereby decreasing available working memory (Buller and Burgoon 1996). When working memory is decreased, people's reaction times also become slower (Unsworth and Engle 2005), and so do hand movements (see also the Stochastic Optimized-Submovement Model in Meyer et al. 1988; Meyer et al. 1990). Namely, when visually guiding the hand to a target, the brain has less time to program corrections to one's movement trajectory. Those corrections result in greater deviations from one's intended trajectory. In other words, movement precision decreases.

One way the brain automatically compensates for decreased precision is to reduce the speed of movements (Meyer et al. 1988; Meyer et al. 1990). Hand (i.e., mouse) movement speed and precision are inversely related (Plamondon and Alimi 1997), so movement precision can only increase if the brain reduces movement speed. In other words, as the body has more time to perceive and program needed corrections, it allows the hand to operate more optimally within the restriction of slower reaction times (Meyer et al. 1988; Meyer et al. 1990). In summary, we hypothesize:

H2: When providing fraudulent responses in an online form, people will exhibit slower mouse speed.

Methodology

To test our hypotheses, we conducted two studies. In Study 1, we used a well-validated visual-perception task that incentivized participants to commit fraud. In particular, participants had to respond to a binary question while we recorded their mouse movements. In Study 2, we used a real-world insurance claim scenario to replicate our results from Study 1 in a more realistic setting. Specifically, we asked participants to complete a sequence of online forms to file automobile insurance claims. While participants completed the forms, we recorded their mouse movements. As in many real-world settings, participants in both studies had freewill to commit fraud in order to boost their compensation—i.e., we did not manipulate or sanction participants' decision to commit fraud in any way. Table 1 provides an overview of the studies.

Table 1. Summary of studies

Study	Methodology	Purpose	Observations	Findings
1	Observational study using an established perceptual task	Test H1 & H2	2158	Fraud influences mouse deviation and speed.
2	Observational study identifying fraud in online claims	Replicate Study 1, improve ecological and external validity	395	Fraud influences mouse deviation and speed.

Study 1: Flexible Dot Task

In Study 1, we show that deception causes changes in mousing behavior. In particular, using a well-established protocol that incentivizes participants to commit fraud, we find that fraudulent behavior increases movement deviation and decreases cursor speed.

Procedure and Material

To examine how fraudulent people move their mouse, we adapted a perceptual task developed by Gino et al. (2010). In this task—sometimes called "flexible dot task" (Hochman et al. 2016)—participants are asked to truthfully identify which side of a square, separated by a diagonal line, contained a larger number of dots. In particular, 20 randomly-generated dots appeared for 1 second in the square—sometimes more on the left side, sometimes more on the right side (see Figure 1 for an example). After the dots disappeared, participants had to select an answer (i.e., "Which side contained more dots?") by moving their mouse cursor to the "left" or "right" selection buttons.

In total, participants completed a sequence of 20 trails. When a trial began, we anchored the mouse cursor in the middle of the screen by requiring the participants to click on a "Start" button. While participants selected their answers, we recorded their mouse movements.

We encouraged participants to commit fraud as follows: Clicking the "right" button always had a higher payout—even when the left side clearly contained more dots—thereby incentivizing participants to click "right" even when the correct answer is "left." In particular, participants would receive 0.5 pence (US¢0.67) for clicking on "more on left" or 5 pence (US¢6.7) for clicking on "more on right." Thus, participants could maximize their payout by fraudulently reporting on all trials that more dots were presented on the right.

The task had four possible outcomes, defined by both the dots' locations (more on left or right) and the participants' choice (clicking left or right) (Hochman et al. 2016). Only one outcome can be considered fraudulent:

1. More dots on left/clicking on left: correct—low payout (*no fraud*—correct reject)
2. More dots on right/clicking on right: correct—high payout (*no fraud*—correct hit)

3. More dots on right/clicking on left: incorrect—low payout (*no fraud*—detrimental error)
4. More dots on left/clicking on right: incorrect—high payout (*fraud*—beneficial error)

Following Hochman et al. (2016), only the beneficial errors could result from attempts to maximize payouts by committing fraud. Consequently, in this study, we compared mouse movements between fraudulent cases (i.e., beneficial errors) and correct responses (either hit or reject), and disregarded detrimental errors.

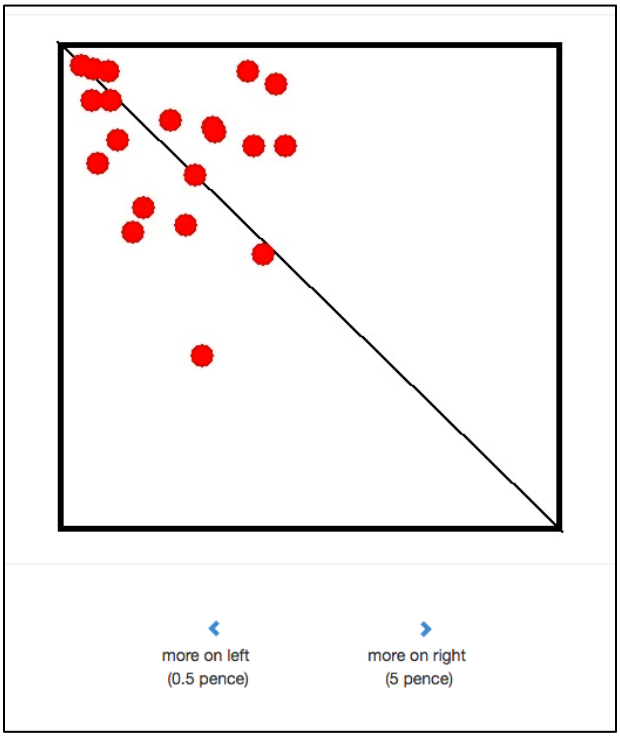

Figure 1. Sample screen from the *flexible dot task* used in Study 1. In each trial, 20 dots were displayed in a square divided by a diagonal. The task was to move the mouse to the correct answer for a given scenario and click on the answer (i.e., to report whether there were more dots on the right or the left side of the diagonal).

Participants

We recruited 150 participants—older than 18 years and from the U.S.—using *Prolific Academic*.[1] The mean age was 30.9 years, and 33.9 % were women. We paid participants £1 for the 10-minute task (equaling a £6/US$8 hourly wage). In line with previous mouse-tracking studies, we eliminated all participants whose completion time was longer than three standard deviations from the average participants' completion time (Freeman and Dale 2013; Selst and Jolicoeur 1994). Further, we excluded anyone who took part on a mobile device, resulting in a sample size of 115 participants with 2,300 observations (each participant was presented with 20 decisions in a repeated-measures design). As we were uninterested in detrimental errors, we excluded those observations from our dataset, resulting in a final sample of 2,158 observations.

Measures

Mouse variables. Mousing data was captured using a webpage-embedded JavaScript library, which captured not only the cursor's x- and y-coordinate pair but also a corresponding timestamp at a millisecond precision rate. Those data were sent to a web service for further processing. First, in line with mouse-movement literature (Hehman et al. 2015), the web service normalized all movements to a standardized 8x6 grid (a ratio consistent with many screen resolutions) to account for different screen resolutions. Second, the web service calculated statistics for deviation and speed.

Deviation was calculated as *actual* distance traveled divided by *optimal* distance (Figure 2). Actual distance was calculated by summing distances between each consecutive x-, y-

[1] Online recruitment platforms have been found to be appropriate for random-sample populations (Berinsky et al. 2012). For example, Mason and Suri (2012) found that the behaviour of respondents on an online recruiting platform closely resembled that of participants in traditional laboratory experiments.

coordinate pair. Optimal distance was calculated as distance between movement's starting and ending point—i.e., a straight line. Thus, the higher the ratio, the greater the deviation per unit moved (normalized pixel). Speed was calculated as actual distance divided by movement time.

Fraud. We coded correct responses (hits or rejects) as 0 and fraudulent cases (i.e., beneficial errors) as 1.

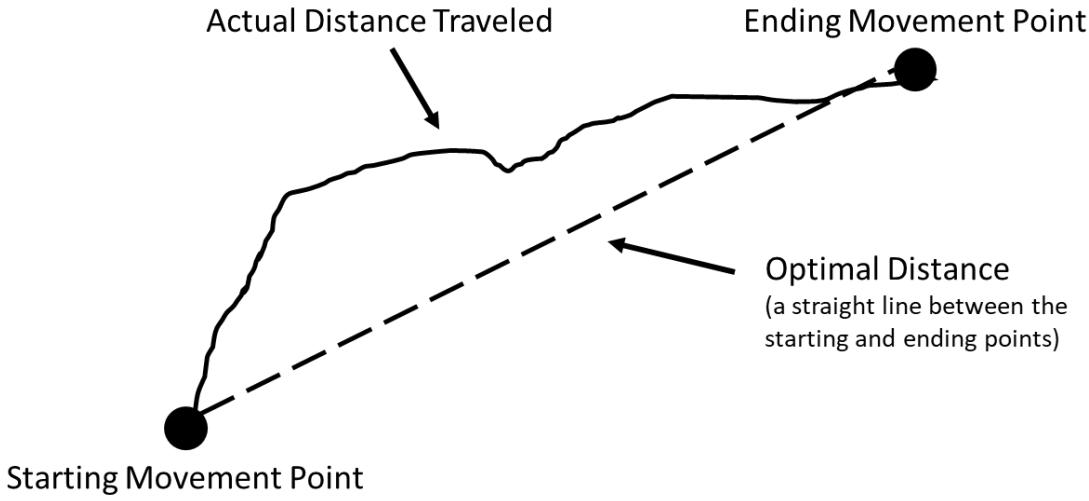

Figure 2. Actual and optimal distances

Model specification

We specified a linear mixed-effects regression model to estimate the effect of fraud—i.e., beneficial error—on our two outcome variables—i.e., mouse-movement deviation (H1) and mouse-movement speed (H2). As such, mixed-effects models account for between-subject variability by allowing individual intercepts to vary. Thus, we specified the following varying-intercept model:

$$Y_{ij} = \beta_0 + \beta_1 \cdot fraud_{ij} + u_{0j} + \varepsilon_{ij},$$

where *i* indicates observations (i.e., each single decision) from *j* participants. *Y* indicates the outcome variables (i.e., mouse-movement deviation and speed), β_0 represents the intercept, and

β_1 is the fixed effect of fraud (i.e., beneficial error). ε_{ij} indicates level-one residuals (i.e., on observation level), which are assumed to be normally distributed with mean 0 and constant variance. As observations *i* from participants *j* might be correlated (i.e., due to the repeated-measures design), we consider a level-two random effect u_{0j} (i.e., on the participant level) that describes the between-subject variability of the outcome variable *Y* and captures the non-independence between observations *i* from the same participants *j*, so it allows the intercept β_0 to vary across subjects (Gelman and Hill 2007). u_{0j} is assumed to be normally distributed with mean 0 and constant variance. We used *R* (Ihaka and Gentleman 1996) with the *lme4* package (Bates et al. 2014) with its *lmer* function to estimate the mixed-effects models.

Results

Of the 2,158 valid observations, 409 (i.e., 19%) were fraudulent. The results show that fraudulent decisions (i.e., when participants made beneficial errors) significantly increase mouse-movement deviation (β_1 = 1.11 p < .001) and decrease mouse-movement speed (β_1 = -.21, p < .05). Table 2 presents the summary statistics for the fraud and mouse variables, and Table 3 presents the results of the models.

Table 2. Summary statistics for Study 1

Statistic	Unit	N	Mean	SD	Min	Max
Fraud						
Dots right (presented)	%	2,158	.47	.50	0	1
Dots right (user clicked)	%	2,158	.66	.48	0	1
Fraud (beneficial errors)	%	409	.19	.39	0	1
Correct hits	%	1,008	.47	.50	0	1
Correct rejects	%	741	.34	.48	0	1
Mouse movement						
Deviation	See text	2,158	5.04	4.68	2.00	100.61
Speed	See text	2,158	3.01	2.00	.68	51.49

Table 3. Mixed-effects regression results for deviation and speed as outcome (Study 1)

	Deviation			Speed		
	Estimate	CI	p-value	Estimate	CI	p-value
Fixed effects						
Fraud (binary)	1.11	.61 – 1.62	.001	-.21	-.40 – -.02	.028
Intercept	4.85	4.54 – 5.16	.001	3.06	2.83 – 3.29	.001
Random effects						
σ^2		20.29			2.59	
$\tau_{00,Participant}$		1.56			1.42	
$N_{Participant}$		115			115	
$ICC_{Participant}$		.07			.35	
Observations		2158			2158	
AIC		12731.94			8463.51	
R^2		.12			.39	

In a further analysis, we used *deviation* and *speed* to infer fraudulent responses (i.e., beneficial errors). We used the set of variables as described earlier in the model specification and consider additional control variables[2], however, in contrast to the first analysis, our outcome variable is now binary. Thus, we used a mixed-effects logistic regression with *deviation* and *speed* as predictors and *fraud* (i.e., beneficial errors) as outcome:

$$Fraud_{ij} = logit^{-1}(\beta_0 + \beta_1 \cdot deviation_{ij} + \beta_2 \cdot speed_{ij} + \gamma' \cdot controls_j + u_{0j} + \varepsilon_{ij})$$

The results show that deviation and speed can be used to infer fraudulent responses (see Table 4). The results indicate that the coefficient for mouse-movement deviation (odds ratio) was significantly greater than "1" (β_1 = 1.04, $p < .01$), consistent with H1 (indicating that greater deviation is correlated with fraud). Further, consistent with H2, the coefficient of the average movement speed (odds ratio) was significantly smaller than "1" (β_2 = .91, $p < .05$) (indicating that slower speed is correlated with fraud). As a measure of goodness of fit, we used Nakagawa

[2] We controlled for age, gender, education, computer usage (hours/week), and internet usage (hours/week).

and Schielzeth (2013) R^2 for generalized linear mixed models[3], using R's *MuMIn* package (Bartoń 2009), leading to an R^2 value of .20. To assess prediction accuracy, we used 10-fold cross validation and achieved virtually the same accuracy, with 82% correctly classified cases.

Table 4. Mixed-effects logistic regression results for deviation and speed as predictors (Study 1)

	Fraud (binary)		
	OR	CI	p-value
Fixed effects			
Deviation	1.04	1.02 – 1.07	.002
Speed	.91	.82 – 1.00	.049
Intercept	.20	.13 – .29	.001
Controls		yes	
Random effects			
$\tau_{00,Participant}$		.63	
$N_{Participant}$		115	
$ICC_{Participant}$		.16	
Observations		2158	
AIC		1996.10	
Deviance		1800.91	

Study 2: Insurance Task

Study 2's purpose was to generalize Study 1's findings. Using an observational study, participants had to file several insurance claims, a task in which people frequently commit fraud (Dionne and Gagné 2002; Miyazaki 2009).

[3] This statistics is defined as $R^2 = \frac{\sigma_f^2 + \sum_{l=1}^{u} \sigma_l^2}{\sigma_f^2 + \sum_{l=1}^{u} \sigma_l^2 + \sigma_e^2 + \sigma_d^2}$, where u is the number of random effects, σ_f^2 is the variance of the fixed effect component, $\sum \sigma_l^2$ is the variance component of the lth random factor (i.e., participants), σ_e^2 is the variance due to additive dispersion, and σ_d^2 is is the distribution-specific variance (Nakagawa and Schielzeth 2013).

Procedure and Material

We asked participants to claim damages to their car—in total, five scenarios[4]—by using an online damage-reporting form (see Table 5 for the scenarios). At the beginning of each scenario, participants received 2,000 coins as play money, and we instructed the participants they would have an insurance contract with a deductible of 600 coins. Recall that contracts with deductibles are often perceived to be unfair (e.g., Miyazaki 2009), so we expected at least some participants to commit fraud (i.e., inflate damages), so as to cover their deductible. We based the five scenarios on scenarios used in a prior study (Hibbeln et al. 2014). To control for learning and sequence effects, we randomized the order of the scenarios.[5]

We designed the damage-reporting form to require mouse input—participants had to mark the damage locations on the rear end of a car (see Figure 3); we started tracking mouse movements upon starting a scenario, and stopped recording at the end of each scenario.

Scenario 2

You had a damage of 800 coins.

The following areas have been damaged.

[4] Using five scenarios in a repeated-measures design allowed us not only to account for between-subject variability, but also to collect enough observations for the statistical analysis.

[5] To induce further variability in fraudulent behavior, we manipulated the likelihood of the fraud being detected and amount of punishment, by randomly assigning participants to one of two conditions—a low punishment with low probability of getting caught (400 coins / 10%) and a high punishment with high probability of getting caught (2000 coins / 50 %). The high punishment / high-probability group reported less damages (3.41 vs. 3.25), though the difference was not significant (-.16; $p = .33$).

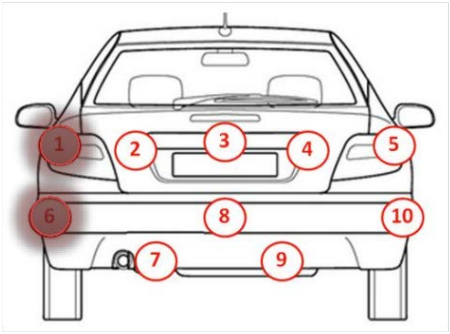

Figure 3. Sample Scenario (Repair Costs: 800; Number of Damages: 2)

Table 5. Overview of scenarios

Scenario #	Repair costs (in coins)	Number of accident damages
1	400	1
2	800	2
3	1200	3
4	1600	4
5	2000	5

Participants

Using Prolific Academic, we recruited 150 participants of at least 18 years of age from the U.S.—mean age was 35.0 years, and 40.5 % were women. We paid £1 for a 10-minute task (equaling a £6/US$8 hourly wage). To ensure that the participant took each scenario serious, we paid a variable bonus for a randomly selected scenario. In particular, for the selected scenario, we paid the claimed repair costs minus the deductible (at a rate of 100 coins/10 pence). Thus, claiming more than the presented damage—committing fraud—resulted in a higher payout, incentivizing participants to commit fraud. In line with Study 1, we excluded not only participants whose completion time was longer than three standard deviations compared to the average participant (Freeman and Dale 2013) but also anyone who took part on a mobile device;

further, we excluded participants whose responses indicated that they did not follow the instructions (i.e., who claimed less damage than presented), resulting in a final sample size of 79 participants with 395 observations (each participant was presented with 5 scenarios).

Measures

Mouse variables. We used the same deviation and speed variables as in Study 1. However, in contrast to Study 1, committing fraud in Study 2 required more mouse movements, as participants had to click more damage locations to commit fraud. Thus, to control for greater deviation resulting from clicking more damages, we calculated an average deviation as follows: First, we segmented each participant's overall movements into sub-movements, where each sub-movement consisted of the movement between each click (e.g., clicking between each damage location; see Figure 5). For each sub-movement, we calculated the deviation; then, we calculated the mean deviation per sub-movement (i.e., the number of damages reported, respectively). This procedure allowed for an unbiased estimate of deviation, an estimate that is unaffected by the requirement to click on more locations to report more damages.

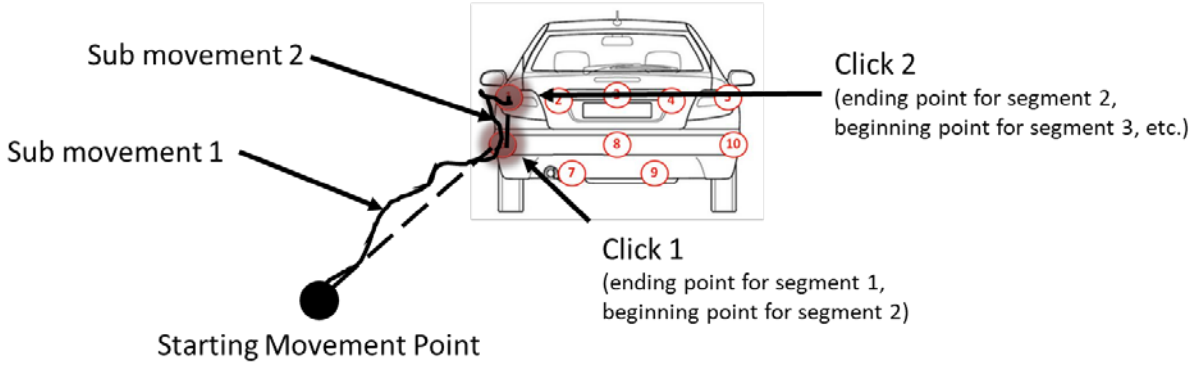

Figure 5. Example of sub-movements

Fraud. In each scenario, participants could choose to commit fraud (or not). In particular, they could claim more damages than presented (see Figure 4). We operationalized fraud as a

binary variable. If the difference between the damages reported and the ones presented in a scenario was positive, we considered it as "fraud" (coded as "1"), otherwise not (coded as "0").[6]

Model Specification

We used the same model specifications as described in Study 1. First, we analyzed the influence of fraud on Y_{ij}, that was mouse-movement deviation and speed, respectively.

$$Y_{ij} = \beta_0 + \beta_1 \cdot fraud_{ij} + u_{0j} + \varepsilon_{ij}$$

Second, we used *deviation* and *speed* to predict *fraud*:

$$Fraud_{ij} = logit^{-1}(\beta_0 + \beta_1 \cdot deviation_{ij} + \beta_2 \cdot speed_{ij} + \gamma' \cdot controls_j + u_{0j} + \varepsilon_{ij})$$

Results

Of the 395 valid observations, 80 (i.e., 20%) were fraudulent. In line with Study 1, the results show that fraudulent decisions (i.e., cases when participants clicked more damage locations than presented) significantly increased mouse-movement deviation (β_1 = 1.25, $p < .01$) and decreased mouse-movement speed (β_1 = -1.59, $p < .01$). Table 6 present the summary statistics for the fraud and mouse variables, and Table 7 presents the results of the models.

Table 6. Summary statistics for Study 2

Statistic	Unit	N	Mean	SD	Min	Max
Fraud						
Damages (presented)	No.	395	3.00	1.42	1	5
Damages (reported)	No.	395	3.32	1.61	1	10
Fraud	%	80	.20	.40	0	1
Mouse movements						
Deviation	See text	395	2.73	3.29	.25	40.86
Speed	See text	395	3.21	4.35	0.61	70.36

[6] We excluded participants from the analysis who reported less than the presented damage, as those had harmed themselves. This is consistent to Study 1, where we also excluded all observations with detrimental errors.

Table 7. Mixed-effects regression results for deviation and speed as outcome (Study 2)

	Deviation			Speed		
	Estimate	CI	p-value	Estimate	CI	p-value
Fixed effects						
Fraud (binary)	1.25	.43 – 2.07	.003	-1.59	-2.68 – -.49	.005
Intercept	2.48	2.10 – 2.86	.001	3.53	3.02 – 4.04	.001
Random effects						
σ^2		10.24			17.88	
$\tau_{00,Participant}$		.37			.76	
$N_{Participant}$		79			79	
$ICC_{Participant}$		.04			.04	
Observation		395			395	
AIC		2060.72			2281.64	
R^2		.12			.13	

In a further analysis, we used *deviation* and *speed* to infer fraud. The results again show that deviation and speed can be used to infer fraud (see Table 8). The results indicate that the coefficient for mouse-movement deviation (odds ratio) was significantly greater than "1" (β_1 = 1.22, $p < .05$), consistent with H1 (indicating that greater deviation is correlated with fraud). Further, consistent with H2, the coefficient of the average movement speed (odds ratio) was significantly smaller than "1" (β_2 = .64, $p < .01$) (indicating that slower speed is correlated with fraud). To assess model fit, we used Nakagawa and Schielzeth's (2013) R^2 for mixed models, leading to an R^2 of .78. To assess prediction accuracy, we used 10-fold cross validation and achieved a comparable accuracy, with 93% correctly classified cases.

Table 8. Mixed-effects logistic regression results for deviation and speed as predictors (Study 2)

	Fraud (binary)		
	OR	CI	p-value
Fixed effects			
Deviation	1.22	1.00 – 1.49	.045
Speed	.64	.46 – .89	.008
Intercept	.09	.00 – .49	.022
Controls		yes	

	Fraud (binary)
Random effects	
$\tau_{00,Participant}$	6.93
$N_{Participant}$	79
$ICC_{Participant}$	.68
Observation	395
AIC	309.25
Deviance	165.29

Discussion

In this paper, we hypothesized how fraud influences both mouse-movement deviation and speed by drawing on the response activation model and two axioms of deception. Using two controlled studies, we not only demonstrated that fraudulent behavior can indeed influence mouse movement but also that such differences can be used to infer fraudulent responses at a high accuracy rate. In particular, we used two tasks—a highly controlled yet artificial task and a real-world insurance claim task—to demonstrate that deceptive people exhibit significantly greater mouse-movement deviation and slower mouse speed.

Theoretical Contributions

In recent years, there has been increasing interest in studying mouse movements within the IS domain; for example, Hibbeln et al. (2017) examined the effects of negative emotion on mouse movements, Grimes et al. (2013) examined the effects of valence and arousal, Jenkins and Valacich (2015) employed mouse movements to examine a system's ease of use, and Anonymous (under review) showed that mouse movements can be used to identify people who conceal information when responding questions in a structured interview. In this research, building on and extending both Hibbeln et al. (2014) and Valacich et al. (2013), we examined the effects of fraudulent behavior on mouse movement. In particular, we derived hypotheses on how fraud influences mouse-cursor deviation and speed by building on two axioms of deception—cognitive dissonance/conflict and cognitive load: When deceiving while completing online forms

using a computer mouse, people experience conflicting cognitions with actionable potential, resulting in deviations of the mouse-cursor path. Further, when deceiving, their brains compensate for a higher load on working memory by adjusting the speed of mouse movements. Using two vastly different studies, we demonstrate that these effects hold, both in a highly contrived and in a more realistic setting. In doing so, we extend extant research on mousing behavior in information systems. In particular, we demonstrate that monitoring and analyzing mouse movements can be used not only to reliably infer emotional states (see Hibbeln et al., 2017), but also cognitive states.

Our work adds to the accumulating evidence of linking hand movements captured through mouse movements to various emotional and cognitive processes (Freeman et al. 2011; Grimes et al. 2013; Hibbeln et al. 2017). What is particularly exciting is that these movements reflect both actual behavior and behavioral changes, measured within an information technology usage context. Our work suggests that analyzing hand movements as an actual (rather than perceptual) measure of usage could enrich other areas of IS research (e.g., technology acceptance, efficacy, fear, etc.), where perceptions of states and behavior are measured post hoc to interaction. Clearly, this approach suggests there are numerous research opportunities.

Practical Contributions

Fraud is ubiquitous and costly in society. As organizations and governments move their processes and forms online, detecting possible deception in those processes and forms is ever more important. This paper proposes a low cost and highly scalable method for detecting possible deception in online forms based on how people interact with online forms via a computer mouse. Capturing mouse movements does not require any special hardware on users'

computers; movements can be collected in a web browser using common and freely available JavaScript libraries such as JQuery. Hence, this research provides theoretically sound and validated cues of fraud that can increase organizations' ability to identify possible fraud in online forms without substantial investment. Arguably, it is impossible to detect fraudulent behavior with complete accuracy, still, organizations could analyze mouse movements that can be used to derive a confidence score and flag suspicious behavior for further auditing. Given that auditing is costly, our procedure makes this process more efficient by allowing companies to focus their scarce resources on those cases that are most likely to be fraudulent. This may result in tremendous savings to organizations, customers, and society in general.

Limitations and Future Research

Like any research, our results come with some limitations. First, our results are limited to a sample population that uses a computer mouse. Given that other input devices have become popular—such as touchscreens and in-air sensors—further research is needed to detect fraud with those devices. Nevertheless, given the strong relationship between cognitive processing and hand movements in the extent literature (Freeman et al., 2011b), our results likely apply to these other devices; our tracking technology ultimately captures the location of any pointing device on the screen (which may include a cursor but also a finger). Further, some of these devices capture even more sophisticated information than does the computer mouse, information that can be used to possibly increase detection accuracy. For example, a touchscreen can capture the diameter of the finger and thereby infer pressure, and in-air sensors capture the z-dimension in addition to the x- and y- dimensions. Future research should explore how human states influence these and other forms of inputs.

Second, besides showing how fraud influences mouse movements, we explored how mouse movements could be used to predict deception. Yet in predicting deception, we relied on only two measures, deviation and speed. Future research should use additional data features to possibly improve prediction accuracy (see Hibbeln et al., 2017); in other words, which other measures—such as acceleration, deceleration, or other movement characteristics—could be related to increased cognitive load or conflicting cognitions?

Third, future research should extend our results to a broader set of contexts and populations. As we sought to test our theoretical explanations, we used two very different studies to test the effect of fraud on mouse movements. Still, we recommend future research to broaden the set of context, so as to further extend the external validity (Dennis and Valacich 2001). Clearly, fraud exists in contexts beyond playing a payout game or submitting insurance claims. Consistent with our theory, we suspect that the results would be amplified when the probability of being caught or punishment severity is increased, as people will be more likely to double check, reconsider, hesitate, or even question their actions.

Conclusion

In this paper, we explored how being deceptive (i.e., fraudulent) in online forms influences mousing behavior. Based on deception theory that connects cognition and hand movements, we posited that being deceptive has physiological and psychological side effects. Those effects can be measured through a computer mouse. Namely, being deceptive results in a user's mouse cursor to not only deviate from its optimal path but also reduce its speed. We tested these hypotheses using two studies. The results of both studies support our hypotheses and suggest that people's mouse movements tend to differ when committing fraud. Our findings have

implications for creating algorithms that detect deception in online forms—as a mass-deployable, cost-effective method for identifying fraud.

References

Bartoń K (2009) Mumin: Multi-Model Inference. R Package, Version 0.12.2 from http://r-forge.r-project.org/projects/mumin/.

Bates D, Mächler M, Bolker B, and Walker S (2014) Fitting Linear Mixed-Effects Models Using Lme4. *Journal of Statistical Software* (67:1):1-51.

Ben-Shakhar G (2012) Current Research and Potential Applications of the Concealed Information Test: An Overview. *Frontiers in Psychology* (3:342).

Buckley JP (2012) Detection of Deception Researchers Needs to Collaborate with Experienced Practitioners. *Journal of Applied Research in Memory and Cognition* (1:2):126-127.

Buller DB, and Burgoon JK (1996) Interpersonal Deception Theory. *Communication Theory* (6:3):203-242.

Carneiro N, Figueira G, and Costa M (2017) A Data Mining Based System for Credit-Card Fraud Detection in E-Tail. *Decision Support Systems* (95):91-101.

Carrión RE, Keenan JP, and Sebanz N (2010) A Truth That's Told with Bad Intent: An Erp Study of Deception. *Cognition* (114:1):105-110.

Clarke M (1990) The Control of Insurance Fraud a Comparative View. *British Journal of Criminology* (30:1):1-23.

Coalition Against Insurance Fraud (2017) The Impact of Insurance Fraud. Accessed November 1, 2013 from http://www.insurancefraud.org/the-impact-of-insurance-fraud.htm.

Coolidge C (2006) Dirty Rotten Scoundrels. Forbes. Accessed November 1, 2013 from http://www.forbes.com/forbes/2006/1016/116.html.

Dale R, Kehoe C, and Spivey MJ (2007) Graded Motor Responses in the Time Course of Categorizing Atypical Exemplars. *Memory & Cognition* (35:1):15-28.

Dean DH (2004) Perceptions of the Ethicality of Consumer Insurance Claim Fraud. *Journal of Business Ethics* (54:1):67-79.

Dennis AR, and Valacich JS (2001) Conducting Experimental Research in Information Systems. *Communications of the Association for Information Systems* (7:1):1-40.

Derrick DC, Jenkins JL, and Nunamaker Jr JF (2011) Design Principles for Special Purpose, Embodied, Conversational Intelligence with Environmental Sensors (Species) Agents. *AIS Transactions on Human-Computer Interaction* (3:2):62-81.

Derrick DC, Meservy TO, Jenkins JL, Burgoon JK, and Nunamaker Jr JF (2013) Detecting Deceptive Chat-Based Communication Using Typing Behavior and Message Cues. *ACM Transactions on Management Information Systems* (4:2):62-81.

Dionne G, and Gagné R (2002) Replacement Cost Endorsement and Opportunistic Fraud in Automobile Insurance. *Journal of Risk and Uncertainty* (24:3):213-230.

Dionne G, Giuliano F, and Picard P (2009) Optimal Auditing with Scoring: Theory and Application to Insurance Fraud. *Management Science* (55:1):58-70.

Freeman JB, and Ambady N (2009) Motions of the Hand Expose the Partial and Parallel Activation of Stereotypes. *Psychological Science* (20:10):1183-1188.

Freeman JB, and Ambady N (2011) When Two Become One: Temporally Dynamic Integration of the Face and Voice. *Journal of Experimental Social Psychology* (47:1):259-263.

Freeman JB, Ambady N, Rule NO, and Johnson KL (2008) Will a Category Cue Attract You? Motor Output Reveals Dynamic Competition across Person Construal. *Journal of Experimental Psychology* (137:4):673-690.

Freeman JB, and Dale R (2013) Assessing Bimodality to Detect the Presence of a Dual Cognitive Process. *Behavior Research Methods* (45:1):83-97.

Freeman JB, Dale R, and Farmer TA (2011) Hand in Motion Reveals Mind in Motion. *Frontiers in Psychology* (2:59).

Gelman A, and Hill J (2007). *Data Analysis Using Regression and Multilevel, Hierarchical Models*, Cambridge University Press: Cambridge, England.

Georgopoulos AP (1990) Neurophysiology of Reaching, in *Attention and Performance Xiii*, M. Jeannerod (ed.), Lawrence Erlbaum Associates Inc.: Hillsdale, NJ, 227-263.

Gino F, Norton M, and Ariely D (2010) The Counterfeit Self: The Deceptive Costs of Faking It. *Psychological Science* (21:5):712–720.

Glover L (2017) 2017 Driving in America Report: The Costs and Risks. Accessed August 24, 2017 from https://www.nerdwallet.com/blog/insurance/state-of-driving/.

Grimes M, Jenkins J, and Valacich J (2013) Exploring the Effect of Arousal and Valence on Mouse Interaction. International Conference on Information Systems, Milan, Italy, December 15-18.

Hehman E, Stolier RM, and Freeman JB (2015) Advanced Mouse-Tracking Analytic Techniques for Enhancing Psychological Science. *Group Processes & Intergroup Relations* (18:3):384-401.

Hibbeln M, Jenkins J, Schneider C, Valacich J, and Weinmann M (2014) Investigating the Effect of Insurance Fraud on Mouse Usage in Human-Computer Interactions. International Conference on Information Systems, Auckland, New Zealand, December 14 - 17.

Hibbeln M, Jenkins JL, Schneider C, Valacich JS, and Weinmann M (2017) How Is Your User Feeling? Inferring Emotion through Human-Computer Interaction Devices. *MIS Quarterly* (41:1):1-21.

Hochman G, Glöckner A, Fiedler S, and Ayal S (2016) “I Can See It in Your Eyes”: Biased Processing and Increased Arousal in Dishonest Responses. *Journal of Behavioral Decision Making* (29:2-3):322-335.

Hunter M (2015) Tax-Refund Fraud to Hit $21 Billion, and There's Little the Irs Can Do. Accessed August 24, 2017 from https://www.cnbc.com/2015/02/11/tax-refund-fraud-to-hit-21-billion-and-theres-little-the-irs-can-do.html.

Ihaka R, and Gentleman R (1996) R: A Language for Data Analysis and Graphics. *Journal of Computational and Graphical Statistics* (5:3):299-314.

Jenkins J, and Valacich J (2015) Behaviorally Measuring Ease-of-Use by Analyzing Users’ Mouse Cursor Movements. Special Interest Group on Human-Computer Interaction, Fort Worth, TX, December 13.

Kulbytė T (2017) 32 Customer Experience Statistics You Need to Know for 2017. Accessed August 24, 2017 from https://www.superoffice.com/blog/customer-experience-statistics/.

Lopez-Rojas EA, and Axelsson S (2016) A Review of Computer Simulation for Fraud Detection Research in Financial Datasets. Future Technologies Conference (FTC), San Francisco, CA, 6-7 Dec, 932-935.

Maehr W (2008). *Emotion: Estimation of User's Emotional State by Mouse Motions*, VDM Verlag: Saarbrücken, Germany.

McKinstry C, Dale R, and Spivey MJ (2008) Action Dynamics Reveal Parallel Competition in Decision Making. *Psychological Science* (19:1):22-24.

Meola A (2016) Online Fraud Attacks in the U.S. Are Growing at an Alarming Rate. Accessed August 24, 2017 from http://www.businessinsider.com/online-fraud-attacks-in-the-us-are-growing-at-an-alarming-rate-2016-4.

Meyer DE, Abrams RA, Kornblum S, Wright CE, and Keith Smith J (1988) Optimality in Human Motor Performance: Ideal Control of Rapid Aimed Movements. *Psychological Review* (95:3):340-370.

Meyer DE, Smith JEK, Kornblum S, Abrams RA, and Wright CE (1990) Speed-Accuracy Tradeoffs in Rapid Aimed Movements: Toward a Theory of Rapid Voluntary Action, in *Attention and Performance Xiv* M. Jeannerod (ed.), Lawrence Erlbaum Associates: Hillsdale, NJ, 173-226.

Miyazaki AD (2009) Perceived Ethicality of Insurance Claim Fraud: Do Higher Deductibles Lead to Lower Ethical Standards? *Journal of Business Ethics* (87:4):589-598.

Morley NJ, Ball LJ, and Ormerod TC (2006) How the Detection of Insurance Fraud Succeeds and Fails. *Psychology, Crime & Law* (12:2):163-180.

Nakagawa S, and Schielzeth H (2013) A General and Simple Method for Obtaining R2 from Generalized Linear Mixed‐Effects Models. *Methods in Ecology and Evolution* (4:2):133-142.

Nunez JM, Casey B, Egner T, Hare T, and Hirsch J (2005) Intentional False Responding Shares Neural Substrates with Response Conflict and Cognitive Control. *Neuroimage* (25:1):267-277.

Palmer CJ, Paton B, Barclay L, and Hohwy J (2013) Equality, Efficiency, and Sufficiency: Responding to Multiple Parameters of Distributive Justice During Charitable Distribution. *Review of Philosophy and Psychology* (4:3):1-16.

Pettey C (2015) The Customer Experience in 2020. Accessed August 24, 2017 from http://www.gartner.com/smarterwithgartner/the-customer-experience-in-2020/.

Plamondon R, and Alimi AM (1997) Speed/Accuracy Trade-Offs in Target-Directed Movements. *Behavioral and Brain Sciences* (20:02):279-303.

Rodrigues M, Gonçalves S, Carneiro D, Novais P, and Fdez-Riverola F (2013) Keystrokes and Clicks: Measuring Stress on E-Learning Students, in *Management Intelligent Systems*, J. Casillas, F. J. Martinez-Lopez, R. Vicari and F. D. l. Prieta (eds.), Springer: Switzerland, 119-126.

Save P, Tiwarekar P, Jain KN, and Mahyavanshi N (2017) A Novel Idea for Credit Card Fraud Detection Using Decision Tree. *International Journal of Computer Applications* (161:13):6-9.

Schiller J (2006) The Impact of Insurance Fraud Detection Systems. *Journal of Risk and Insurance* (73:3):421-438.

Selst MV, and Jolicoeur P (1994) A Solution to the Effect of Sample Size on Outlier Elimination. *The Quarterly Journal of Experimental Psychology* (47:3):631-650.

Sip KE, Roepstorff A, McGregor W, and Frith CD (2008) Detecting Deception: The Scope and Limits. *Trends in Cognitive Sciences* (12:2):48-53.

Smith BD (2000) Insurance Fraud Should Be Everyone's Concern. *CPCU Journal* (53:3):137–138.

Song JH, and Nakayama K (2008) Target Selection in Visual Search as Revealed by Movement Trajectories. *Vision Research* (48:7):853-861.

Sorrell S (2017) Online Payment Fraud, 2016-2020. Juniperresearch.Com. Accessed August 24, 2017 from http://www.experian.com/assets/decision-analytics/white-papers/juniper-research-online-payment-fraud-wp-2016.pdf.

Unsworth N, and Engle RW (2005) Individual Differences in Working Memory Capacity and Learning: Evidence from the Serial Reaction Time Task. *Memory & Cognition* (33:2):213-220.

Valacich JS, Jenkins JL, Nunamaker Jr JF, Hariri S, and Howie J (2013) Identifying Insider Threats through Monitoring Mouse Movements in Concealed Information Tests. HICSS-46 Symposium on Credibility Assessment and Information Quality in Government and Business, Maui, Hawaii, January 7 - 10.

Vuitton E (2017) Ecommerce Payment Fraud Outlook 2017-2020. Accessed August 24, 2017 from https://chargeback.com/ecommerce-payment-fraud-outlook-2020/

Welsh TN, and Elliott D (2004) Movement Trajectories in the Presence of a Distracting Stimulus: Evidence for a Response Activation Model of Selective Reaching. *The Quarterly Journal of Experimental Psychology* (57:6):1031-1057.

Zimmermann P, Gomez P, Danuser B, and Schär S (2006) Extending Usability: Putting Affect into the User-Experience. Proceedings of NordiCHI'062006, 27-32.

Zimmermann P, Guttormsen S, Danuser B, and Gomez P (2003) Affective Computing-a Rationale for Measuring Mood with Mouse and Keyboard. *International Journal of Occupational Safety and Ergonomics* (9:4):539-551.

Appendix A: Study instructions

Study 1: Instructions flexible dot task

Your task:

- You will see a box with multiple red dots in it (see example below).
- You will only see the dots for about 1 second, and once they disappear your task is to indicate whether there were more dots on the right side of the square or on the left side of the square by clicking on the left or right button (note that sometimes a dot will be on the line between the two parts).
- In total, we present you 30 trials. 10 practice trials and 20 real trials to earn money.
- This study is expected to take approximately 10 minutes to complete.
- Your participation is completely voluntary and you may quit the study at any time.

Payment:

- To motivate your efforts, we will pay you based on the buttons you click (not based on whether you are correct or not)!
- Because most people can more easily estimate the number of dots on the left side, we will pay you 0.5 pence for each trial that you answer as having more dots on the left side, and 5 pence for each trial that you answer as having more dots on the right side (see illustration).

Figure A1. Flexible dot study instructions sheet

Study 2: Instruction insurance task

Situation:

- You have an **initial wealth of 2,000 coins**.
- For your vehicle, you purchased an **insurance policy with a deductible of 600 coins**. In other words, if the damage to your car was 1,000 coins, you would be responsible for paying the first 600 coins, and the insurance company would pay the remaining 400 coins.
- Imagine that recently, you had an **accident** when backing up into a small parking spot, and **damaged the rear end of your car**.
- Now, you have to **file an insurance claim** on the **insurance company's website**.

Example:

- Before the accident, you have an initial wealth of 2,000 coins.
- The repair of the damage to your vehicle costs 1,000 coins; thus, your wealth is reduced to 1,000 coins.
- Assume you file a claim of 1,300 coins. Given your deductible of 600 coins, the insurance would pay you 700 coins (1,300 coins – 600 coins).
- Your final wealth after receiving payment from the insurance company would be 1,700 coins.

Your task:

- You will be presented with 5 different scenarios, for which you will have to file insurance claims. In each scenario, the damage to your vehicle is different.
    - In each scenario, you have an initial wealth of 2,000 coins. The higher your claim, the higher the payment from the insurance company. In other words, **your final wealth depends on the amount you claim from the insurance company**.

- Group 1: The insurance company screens 10 % of all insurance claims. When the insurance company detects cheating by the insured, this leads to a punishment of 400 coins.
- Group 2: The insurance company screens 50 % of all insurance claims. When the insurance company detects cheating by the insured, this leads to a punishment of 2,000 coins.

Please note:

- Please make sure that you understand the instructions provided. All answers provided in this study are strictly anonymous.

Figure A2. Insurance study instructions sheet