The current issue and full text archive of this journal is available at
www.emeraldinsight.com/1834-7649.htm

Rogue insiders, signature loopholes, and fraud rings

Lessons learned by a Chinese B2B mogul

Chengqi (Chen) Guo
Computer Information Systems & Business Analytics, James Madison University, Harrisonburg, Virginia, USA, and
Xiaorui Hu
Decision Sciences and Information Technology Management, Saint Louis University, Saint Louis, Missouri, USA

Abstract

Purpose – The purpose of this paper is to report the findings and lessons learned from a case study that is based on Alibaba's business-to-business (B2B) fraud in China. The influence of such incidents and post-hoc solutions are research worthy in today's booming digital business world.

Design/methodology/approach – The paper uses a case study approach and practice-driven method that rely on user behaviors, corporate policies, and financial data. The taxonomic framework of online fraud and corresponding countermeasures arise from digital forensic reports, policy reviews, data analysis, and a literature review.

Findings – The key findings are indigenous to the Chinese B2B landscape, yet they help international stakeholders understand and address fraudulent issues. The paper finds beside the traditional customer-based account signature, internal employees must be assigned their own signature systems to track malicious activities. Meanwhile, digital signature systems can be enhanced by reducing the record inter-arrival time. Policy revisions are proposed to (e.g. offshore companies) lead to the decrease in the number of fraudulent incidents.

Originality/value – The paper extends existing understanding of online fraud by studying a Chinese case. The findings are timely and based on real world experience. Actual practices are discussed and evaluated. A range of fraudulent activities is reviewed in a comprehensive framework. The findings are important due to the public exposure and wide implications of such an incident. Also, this study reveals that fraud protection is an on-going effort requiring a triangulation of technical artifacts, policy management, and operations management.

Keywords Online fraud, E-commerce security, B2B, Internal threat, Alibaba, Cyber crime, Crimes, Electronic commerce, China, Fraud

Paper type Research paper

Introduction

Trust, the cornerstone of online trading, is constantly challenged by various means. It is nothing new to say that online fraud is an important, yet loathed, phenomenon in our e-commerce society. A surge of online fraud and consumer deceptions have accompanied the proliferation of electronic business (Xiao and Benbasat, 2011). According to the Internet Crime Complaint Center (IC3), a government agency that continuously monitors the development of internet-related fraud complaints, online fraud is a multi-billion dollar global "business." The Association of Certified Fraud Examiners (ACFE, 2010) reported that US companies would lose an estimated 8 percent of their annual revenues to fraud. A typical wire transfer fraud is estimated to cause

International Journal of Accounting and Information Management
Vol. 20 No. 4, 2012
pp. 348-362

1834-7649
DOI 10.1108/18347641211272704

financial losses averaging $100,000-200,000 per victim (McGlasson, 2010). The form of online fraud also continues to change. As pointed out by RSA, the Security Division of EMC Corporation, online fraud rings have evolved to match those of the legitimate business paradigm. They provide "fraud-as-a-service," which is a highly automatic, easy to use process that enables people with little knowledge and skills in computer networking and programming to commit fraud (RSA, 2010).

The current literature of online fraud covers a wide variety of fraud detection methods and designs, including organizational auditing, data mining applications, and neural network-based predictive tools (Kochetova-Kozloski *et al.*, 2011; Adepoju and Alhassan, 2010; Edge and Sampaio, 2009; Viaene *et al.*, 2005; Rotem, 2011; Choo, 2011; Owhoso and Weickgenannt, 2010). Although prior research has investigated multiple levels of fraud, such as at the corporate level (Mieke *et al.*, 2010), the individual level (Sadan and Schwartz, 2010), the financial sectors (Reffett, 2010), tax auditing (Tomasic, 2011), and social issues (Laufer and Betzer, 2010), more research is needed to provide insights on internal threats and practice-driven studies (Choo, 2011), which are valuable for establishing real time, effective, and interactive preventive strategies against e-commerce fraudulent activities.

Our study provides original value to the literature and practice in several ways. First, indigenous practices are discussed and evaluated. Second, as rogue insiders have become an increasingly popular cause of today's e-commerce frauds (Boss *et al.*, 2009), our study propose solutions to such issues. Third, the purpose of fraud predictive techniques covered by prior research is to pinpoint or classify whether an instance is fraudulent or not, however, our study focuses on a real world incident, and we believe that descriptive case analysis is a suitable and more appropriate method for this research. The descriptive case analysis provides us with insights on the comprehensive scope of observation beyond the single concern – fraudulent or not. As a well-established research approach (Lee, 1989), descriptive case analysis brings us to an understanding of a complex issue by emphasizing detailed contextual analysis. This paper also provides an understanding of indigenous Chinese business-to-business (B2B) issues that stakeholders need to address. China has been experiencing rapid economic growth and an unbalanced development of information communications technology (ICT). These digital gaps are conspicuous in Chinese society, resulting in an unequal access to information. For example, local businesses in rural areas, where high speed internet is not available, can be victims of identity theft. Malicious vendors who have better access to information may commit fraud with stolen identities, making crime investigation difficult if not impossible. Meanwhile, service providers including Alibaba have been relying on non-ICT methods (e.g. door-to-door interviews) to acquire customers in rural areas. Although effective, such methods allow rogue insiders and malicious vendors to collaborate in fraudulent crimes. A lack of legislative protections for online traders also leads to the proliferations of e-business fraud in China. Therefore, deeper insight is needed to uncover the intrinsic factors that are part of the scam.

This study aims to provide practice-oriented suggestions (e.g. account signature updating) for both scholars and practitioners to better understand and execute countermeasures of e-commerce fraud. The context of this study is specific to online B2B platforms, an area that suffers significantly from fraudulent activities and financial losses. Based on the investigation of frauds at Alibaba, the authors attempt to address several issues in the following areas: member screening processes, internal controls, and collaboration with government agencies. In addition, this paper proposes a taxonomic

framework that comprehensively illustrates and categorizes the most recent developments of fraudulent crimes in Chinese B2B markets. This paper also depicts a typical fraud ring that has damaged the reputations of many legitimate electronic businesses. Finally, our study suggests remedial measures and lessons learned that have yielded initial promising results.

In the following sections, we explain the background of Alibaba, the latent fraudulent clusters, the forensics data, the compromised loopholes, the *post hoc* measures, and the evaluations. Although our study is practice-driven, it can be utilized to provide a theoretical grasp of the B2B phenomenon of fraud by identifying the motivations and opportunities for committing fraud, and by providing the various avenues for fighting it.

Backgrounds

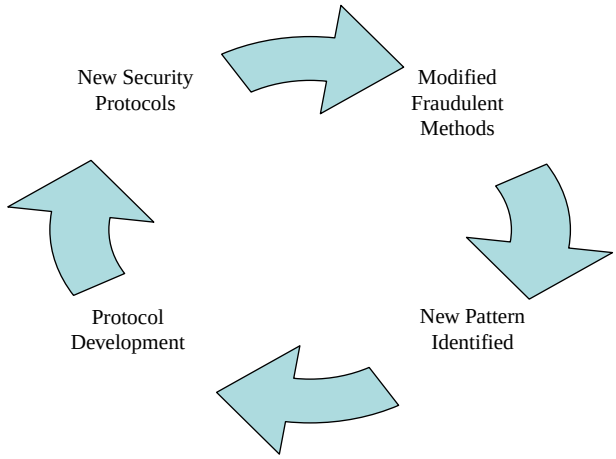
With the gradual recovery of the Chinese economy and supportive government policies, the Chinese online B2B markets are booming. Currently, over 10,000 B2B web sites are operating, and the daily updates of product information exceed three million items. Alibaba Group Ltd, founded in 1999, is undoubtedly the largest internet trading company in China. It has been recognized by *Forbes* magazine as the "World's Best B2B Platform" for six consecutive years. Its founder, Mr Jack Ma, was the first Chinese entrepreneur in 50 years to appear on the cover of *Forbes* magazine.

The Alibaba Group includes seven companies and other affiliated entities: Alibaba.com, a B2B e-commerce platform for small businesses; Taobao Marketplace, a C2C platform for customers; Taobao Mall, a B2C platform; eTao, a comprehensive shopping search engine; Alibaba Cloud Computing, an advanced data-centric cloud computing service; China Yahoo!, an internet portal; and Alipay, a trusted third-party online payment platform. Among these, the B2B platform is the most popular among the small businesses around the world.

Alibaba.com provides software, technology, and services that connect small and medium-sized buyers and suppliers, as well as internet content, advertising, business management software, and internet infrastructure services. Alibaba attracts and matches buyers and suppliers around the world to do business through their three online marketplaces: a global trade platform (www.alibaba.com) for international importers and exporters, a domestic platform (www.1688.com), and a transaction-based wholesale platform on a global site (www.aliexpress.com). With these three marketplaces, Alibaba proudly boasts a community of around 72.8 million registered users in more than 240 countries and regions; offices in more than 70 cities across China, India, Japan, Korea, Europe and the USA; and over 23,000 employees around the world.

Discovery and investigations of the fraud

Despite the continuous efforts of online fraud mitigation, criminals react and adapt at an incredible speed, as Figure 1 shows. When facing state-of-the-art security protocols and countermeasures, criminals adapt by seeking a different approach to committing fraud, as demonstrated in the Alibaba B2B fraud case. The Alibaba Company first found a surge in the number of fraud complaints toward the B2B marketplace in October 2010. An internal investigation immediately followed, and they discovered that more than 1,000 fraud cases had been reported in both 2009 and 2010. Further investigation was conducted and revealed the pattern of the fraud and was able to pin down a group of suspicious sellers. A case was then filed with the Hangzhou Police Department



Source: Adapted from Edge and Sampaio (2009)

Figure 1.
The development lifecycle of fraudulent activities

in February 2011. With the full cooperation and support of Alibaba and the dedication of the Chinese police force, this international criminal case, involving more than $6.6 million, was solved within two months. By April 11, 2011, 36 suspects were detained and all 19 major suspects were arrested.

According to the *Wall Street Journal* (2011):

> [. . .] police in eastern China have detained 36 people in an investigation of fraudulent listings on online trade platform Alibaba.com Ltd, the latest development in a scandal that triggered an overhaul at Chinese largest e-commerce company and the departure of its chief executive.

In this incident, more than 100 sellers' accounts were created using false personal and business identities. The criminals allegedly collected about $6.6 million from the victims through international money mules without actually shipping the promised products.

More than six gigabytes of digital forensics data were collected, and over 130 bank accounts were revealed to be associated with the Alibaba B2B fraud perpetrators. Victims were primarily from North America (Figure 2) and they were attracted to the fraudulent suppliers due to the low prices and the trustworthy status, Gold Supplier, assured by Alibaba.com. Fraud perpetrators obtained Gold Supplier certificates through rogue insiders by offering financial returns. Such an issue calls for both service agreement revisions and enhanced internal controls. Meanwhile, over 100 of Alibaba's sales representatives, out of the sales workforce of 5,000, were fired for their alleged involvement in the fraud (*BBC News*, 2011). Those sales representatives were found to have colluded with more than 2,300 sellers to create fraudulent listings and to allow those sellers to trade without proper authentication and verification measures. This incident reveals the lack of ethical conduct from the insiders and the dark side of the e-commerce markets in China.

Moreover, through cracking this case, Chinese police found that criminals have formed an underground fraud ring, or fraud-as-a-service, to commit frauds across various e-commerce platforms. The illegal services included trading platform accounts,

Figure 2.
The global reach of Alibaba B2B fraud

trading fake identifications, opening fraudulent bank and communication accounts, facilitating the deposit and withdraw of fraudulent funds, etc. As the framework in Table I indicates, there is a wide range of fraudulent activities plaguing the landscape of Chinese e-commerce. We believe that if these activities are not well controlled, they will not only damage the Chinese online marketplaces, but they will also negatively impact the global online environment. From this incident, we see a call for global cooperation to fight these crimes.

Findings and lessons learned for fighting B2B fraud

Although new patterns of fraud continue to rise, most incidents today are simply "the same wine with a different bottle." Currently, utilizing a combination of tricks to target a large uninformed audience, the criminals still successfully manage to pull off some of their schemes. The data collection and analysis in this study is mainly *post hoc*. Most data come from industrial reports by Alibaba and the online fraud literature. Using a method of content/context analysis, we have discovered the following findings. First, compared to the USA, China has a significantly lower rate of reported fraud complaints. The USA has been ranked the number one nation for receiving the most individual complaints of online fraud, followed by Canada, the UK, and Australia (IC3, 2011). However, this lower rate should not lead to the conclusion that the Chinese online trust system is better. This lower rate can be attributed to the infancy of Chinese e-commerce penetration and the lack of awareness of the available online fraud protections. Second, the most effective B2B frauds appear to have the following common characteristics: highly mobile teams, a small scale of personnel, a clear segregation of functional units, and cross region/country operations. Third, there is a lack of account profiling systems (e.g. digital signature driven profiles) based on employees' work behavior at Alibaba, thus creating a loophole for rogue insiders to bypass organizational policy to assist in fraud. There is a lack of non-repudiation features in the old security system, and such a limitation was exploited by perpetrators in Alibaba's case. Fourth, compromised insiders have definitely become a significant enabler in today's digital crimes. Fifth, online fraud cannot be eradicated through the use of technology alone. The concept

Fraud	Description	Major security protocol	Frequency	Popular profile of victim
Lottery scheme	Victims receive lottery winning message through e-mail, IM, or forums, which ask them to wire income tax or deposit to their money mule account	Cross reference Safeguard confidential/private information	Frequent	Small businesses Individuals
Low price offer	Extremely low product price is offered to victims. Once the first purchase is made, fake or empty merchandise is delivered	Never process any payments prior to receiving merchandise Cross reference	Most frequent	Small businesses Individuals
Stock options scheme	By forging government documents and establishing off-shore companies, criminals solicit funds from victims by branding themselves as attractive investment stock options	Cross reference Visit blacklist database such as ChinaNet110.com	Moderate	Start-up companies Small businesses
Mutual funds scheme	Criminals pretend to be from an oversea investment agency that offers "insider information" to members, who pay high monthly membership fees and receive invaluable investment advice	Cross reference Visit blacklist database such as ChinaNet110.com	Moderate	Start-up companies Small businesses
Spear phishing	Using e-mail spoofing to target specific victims, criminals seek unauthorized access to confidential data. Perpetrators are after trade secrets, intellectual properties, and patents	Invest on information technology (IT) security solutions Harden computer and network environment	Most frequent	Small businesses
TV show scheme	Perpetrators use forged identifications to offer TV commercial breaks with lucrative fees much lower than those of legitimate programs	Cross reference Visit blacklist database such as ChinaNet110.com	Moderate	Start-up companies Small businesses
Pyramid selling	By offering fake job ads or auction bids, criminals attempt to develop off-line multi-level marketing with victims who suffer from financial losses due to unfair contract terms	Cross reference Visit blacklist database such as ChinaNet110.com	Less frequent	Individuals Small businesses Start-up companies
Off-shore scheme	Perpetrators utilize the brand of an oversea ghost firm to launch frauds such as stock option and mutual fund schemes	Refer to blacklist database Require international collaborations	Frequent	Individuals Small businesses Start-up companies
Free sample scheme	Victims pay shipping and handling fees for "free" samples	Do not make any payment before receiving merchandise	Moderate	Individuals Small businesses

Table I.
A taxonomic framework of major Chinese B2B fraudulent activities

of the digital certificate, such as the Gold Membership, was introduced to Alibaba's trading system when the company was first founded, yet, it was easily manipulated by rogue insiders. Although the dual signature system (e.g. a digital signature system tracking behavior of both employees and clients) suggested by this study is argued to be a viable solution, managerial intervention cannot be overlooked.

The B2B frauds have evolved into a highly profitable sector that requires specified knowledge and training. According to the investigation, the perpetrators of Alibaba fraud have at least bachelor degrees, are savvy in computer/network technologies, are fluent in multiple languages, and are well organized into teams. As Figure 3 shows, perpetrators took advantage of the loopholes in the signature system, the bank account management system, computer networks, and insider incentives, to lay the foundation that support their fraudulent schemes. Without the help of those insiders, even though the fraud might still be able to be successfully committed, it would be with much greater difficulty.

Many issues have been discovered inside Alibaba, and important lessons could be shared amongst stakeholders. In general, these lessons are divided into two sectors: before transaction and after transaction:

(1) *Pre-transaction activities*:
- Establish and enable profile-based signature system for employees.
- Cross reference the behavioral models of customers, members, and employees.
- Strengthen member admission policy. Screen out unreliable vendors.
- Strengthen hiring process. Establish reference-based network for sales representatives.

(2) *Post-transaction activities*:
- Timely update employee and member signatures with new transcations.
- Cross reference with blacklist database on regular basis.
- Mitigate insider threat by motivating and educating employees about business ethics.

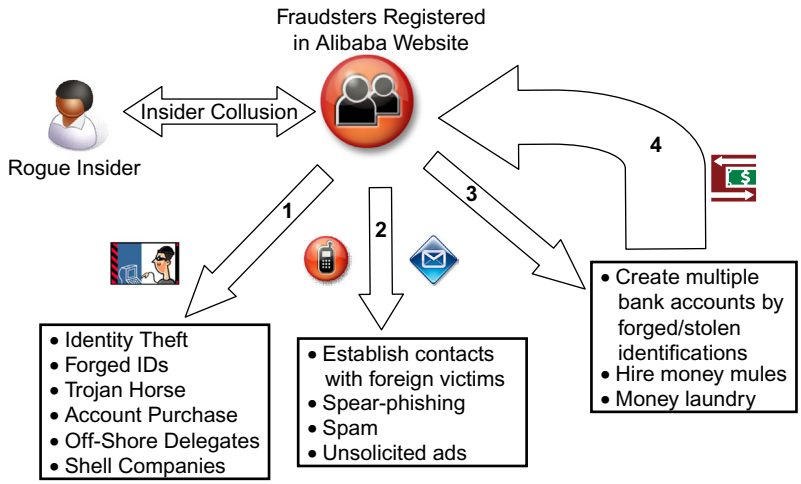


Figure 3.
How Alibaba scam works

- Eliminate members with negative indicator (e.g. fraudiness score) of fraudulent activities. The indicator typically includes both qualitative and quantitative measures; both should be evaluated thoroughly prior to decision making.

In this way, a sequence of activities can be presented. For example, establishing profile-based signatures of employees should occur prior to that of customers. A black list of malicious vendors should be developed by cross checking member's behavioral models. Further, since many fraudulent activities are well prepared prior to business transactions, pre-transaction actions should focus on preventive measures that mitigate the possibility of malicious member vendors. As a result of this incident, Alibaba has raised the standards for the approval of suppliers by enforcing an enhanced Gold Supplier™ Service Agreement. New digital verification and authentication systems are being used along with a new supplier validation process, which requires staff to visit and interview off-site stores on a regular basis. Combined with employee-side internal controls, enhanced validation procedures minimize the possibility that malicious vendors can collaborate with rogue employees to obtain unauthorized Gold Supplier certificates. Alibaba's remedial measures also need to include signature monitoring procedures to develop a pattern-based data network that not only tracks the behavior of the members, but also the actions of employees who constantly interact with e-vendors. In this way, a stronger non-repudiation feature of the security measure is strengthened. Post-transaction, on the other hand, focuses on data collection and analysis for generating a behavioral pattern of stakeholders. Aside from the technical aspects of the countermeasures, traditional methods of workshops, focus groups, and field studies can be used to promote the awareness of business ethics amongst internal employees.

More specifically, practitioners should adhere to the suggestions in these two domains: practice development and stakeholder management. The second domain is directly influenced by the first one through IT activities, performance metrics, internal controls, the Central Intelligence Agency (CIA) and strategic concerns (Table II). Investment in IT solutions has become a common resort in today's business environment. As discussed earlier, signature models have been proven to be an essential avenue in predicting malicious behavior (Edge and Sampaio, 2009). These models can play an active role in B2B transactions to protect the interests of legitimate stakeholders. It is suggested in this paper that signatures must be adopted by both member vendors as well as employees. Rogue insiders could generate income by selling unauthorized digital certificates, Golden Member for example, to otherwise disqualified vendors, who conduct fraudulent activities to obtain financial gains. Confidential data, such as contact lists, could be traded by employees to fraud perpetrators for social engineering attacks and identity thefts. If employee-side signature is enforced, their behavior would be tracked and monitored. Studies have shown that employees will follow protocols more effectively if they think they are watched. Another noteworthy issue lies in the strategic concerns of Alibaba. A more rigorous entrance standard set for the suppliers might lead to a short-term reduction in revenue and sales volume; however, ethical integrity and a good company reputation will pay off in the long run, as indicated by previous studies. Leading by example and setting a higher standard for the industry should be the pioneer's mission. In fact, Google is trying to expand its B2B sector that competes with Alibaba, which is pushing the Chinese B2B giant to strengthen its consumer trust (*Business Week*, 2011). In response to the scam complaints, Alibaba has established a compensation mechanism that aims to promote trust in the site

Characteristic	Practice development	Stakeholder management
IT activities	Designing, acquiring, building, enhancing, and maintaining signature score information systems for internal employees, members, and customers	Establish strategic alliances with third party organizations (e.g. ChinaNet110) Create and share violators' signature with business justice entities Develop partnership with Chinese B2B research center
Performance metrics	Adding signature-based scores to gauge employee reactions to policy changes	Diversify incentive mechanisms by incorporating clean fraudiness score Evaluate both quantitative and qualitative performance measurement Offer ambitious yet reachable sales thresholds and bonus incentives to representatives
Internal control (employees)	Creating network of references. Adding background check to hiring process. Monitoring employee behavior through objective/subjective measurements	Require insider employees to comply with pre-incident planning and communications Provide continuous support to internal threats management Perform onsite tasks that require processing granularity Regulate and monitor transaction rate β so as to enforce accurate signature update
Confidentiality, integrity, and availability	Offering third party payment protection programs (e.g. AliPay). Outsourcing data cryptography and backup services. Applying corporate intranet/extranet security solutions	Build blacklist database for suppliers, members, and customers Limited to development stakeholders Broadly concerned with access control to physical devices, data, and operating systems
Strategic concerns	Forbidding the registration of off-shore delegates. Forbidding personal membership. Enforcing more rigorous entrance barrier. Forbidding re-assignment of active contracts that do not terminate with natural or legitimate causes. Providing insurance plans as damage control approach to mitigate the impacts of fraudulent activities	Monitor account activities to avoid identity theft or replication Restrict contract auctions Require authentications to every legitimate online supplier Regulate advertisement publishing and information disclosure Promote the awareness and understanding of tightened membership management

Table II.
Post-incident practice development and stakeholder management

and to alleviate customer's losses. So far a total of $2 million in compensation has been given to Chinese and international victims of this B2B fraud incident. More compensation will follow. Meanwhile, a call for government intervention is necessary in both the short- and long-term strategic plans. The very action of Alibaba to involve the government in the investigation led to the success of the investigation and a timely halt of the criminal activities. Practice development and stakeholder management were compiled and reviewed after the incident. Table II is rooted in two suggested changes that aim to fix the flaws in Alibaba's original B2B infrastructure: stakeholder's signature and insider threats.

Meanwhile, Alibaba has provided practical guidelines to its customers. Many online educational materials, including online news, forums, and videos, can be freely accessed

by buyers and sellers to enhance their knowledge. Specific guidelines and advice on how to protect oneself are also offered, such as the following: be wary of extremely low prices; view sellers' credit and the quality of goods before making a purchase decision; use safe Paypal and U Shield, etc. as payment instruments; protect personal identification numbers, account numbers and passwords, and other private and important information; and avoid the use of internet cafes and other public access points to conduct e-commerce related activities. With the assistance of law enforcement entities, Alibaba's *post hoc* remedies appear to be effective. Alibaba fraud complaints have been reduced nearly 70 percent and the number of malicious vendors is down to a single digit.

Signature models

Account profiling has been widely utilized by financial sectors, credit unions, and government agencies, largely due to its straightforward threshold values and process granularity. Customer signatures are often analyzed to track legitimate account activities through behavioral variables that reflect updating transactions, which in turn can be used to sketch a pattern of user behavior. When Alibaba's employees try to acquire new service subscribers in rural areas, a traditional onsite "door-to-door" method is used. Such a method creates potential problems. For instance, in order to make more commission by acquiring new subscribers, employees loan or sell digital signatures of premium memberships to vendors who are not qualified to own such titles. On the other hand, vendors may conceal important information (e.g. debt-to-asset ratios) from Alibaba to avoid inspection. A client-side signature has been widely used by today's e-business providers, including Alibaba, however, a lack of internal controls has been proven to be effective at jeopardizing the entire system. In a legitimate digital signature system, internal employees may hijack the authentication mechanism and profile screening process. Therefore, we propose an approach (e.g. a dual signature system) that utilizes a digital signature to monitor not only clients but also employees.

Signatures are mostly generated through linear programming or regression models, such as Cahill *et al.* (2000), Ferreira *et al.* (2006) and Cortes and Pregibon (2001). Take Ferreira *et al.* (2006) as an example (Figure 4), $\boldsymbol{S_{t+1}}$ is the new signature while $\boldsymbol{S_t}$ is the current signature. β allows us to evaluate the effect of new actions P_c on the existing signature value (S_t). β and $(1 - \beta)$ are assigned weights of the old signature score S_t and the newly occurred transaction (P_c). Given the values of β, one can determine how fast the old data become expired. Cahill *et al.* (2000) (Figure 5) proposed a probability model that is capable of predicting the chances of having a fraudulent account. The model indicates F as the fraud signature and A as the account signature, thus generating an indicator for suspicious instances that appear unexpected under a normal account but expected under a fraudulent account. Cortes and Pregibon (2001) further suggested a

$$S_{t+1} = \beta.\ S_t + (1 - \beta).\ P_c$$

Figure 4.
A linear weighting function by Ferreira *et al.* (2006)

$$C_{n+1} = \log(F(X_{n+1})/A_{n+1}(X_{n+1}))\ P_c$$

Figure 5.
Probability of new account behavior estimate by Cahill *et al.* (2000)

model to determine significant deviation within customer signatures that may represent a fraud, as shown in Figure 6.

Practice wise, a common pitfall of account profiling is the over reliance on digital signatures. In fact, signature systems require accurate and consistent human interventions in order to be effective. It must be kept in mind that several inputs of the model come from business processes and rules, which are highly dependent on human interventions. Human observation and interference should not be taken lightly. Constant efforts must be ensured in the processes of transaction updates and score calculations. For example, β can be determined by an experienced data analyst or a project supervisor, but it can also serve as a dependent variable in the function of the record inter-arrival time. Therefore, the smaller the interval, the more agile β yields, which relies on the frequency of observations by internal employees. In Alibaba's case, a monitory system can be used to enforce a minimal time interval of record entry.

There is a variety of signature products in the market. Each company may adopt what seems to have the best fit. The above examples illustrate how internal controls can be strengthened by using employee-side signatures, which require constant human interventions. The behaviors of employees must be monitored, although with different standards, along with the clients. Doing so could mitigate the chance of joint fraudulent activities by both insiders and vendors.

Insider threats

Empirical findings have been made in previous studies on how internal threats are compromising corporate IT security (Boss *et al.*, 2009; Hu *et al.*, 2007; Dhillon, 2001). In the Alibaba incident, the rogue insiders from sales departments hijacked the validation process of off-site vendors by taking commissions from outside perpetrators. More than 100 sales representatives were directly involved with fraudulent operations, such as admitting members without background checks, releasing confidential information to perpetrators, and forging fake documents of lost merchandise. Therefore, a diversified strategy must address insider threats from both the technical and non-technical perspectives, as indicated in Table III. A critical finding lies in the signature loophole of Alibaba's authentication system, which did not incorporate an employee signature model. Hence, we suggest a dual signature system that counteracts daily changing fraudulent schemes in the Chinese B2B landscape. As many studies pointed out, individual perceptions of the required controls (e.g. a behavior-based signature) are a significant part of information security management (Choudhury and Sabherwal, 2003). Research also suggests that a lack of visual cues in communication leads to a higher chance of successful frauds because people are more vulnerable to strategic manipulation in a non-face-to-face interaction (Short *et al.*, 1976). Today's e-business often requires minimal visual cues; instead, asymmetric communications including fax, e-mail, and instant messaging are extremely popular. Such trends enable perpetrators to customize their strategies to a wide spectrum of audiences, including insiders of legitimate businesses. Therefore, internal controls must be updated on a regular basis.

An interesting phenomenon is that outside perpetrators are found to be well educated and highly skilled in computer technology, foreign languages, and business

$$\text{Fraudiness} = \frac{\text{prob (customer signature)}}{\text{prob (fraudster signature)}}$$

Figure 6.
Fraudiness scoring model by Cortes and Pregibon (2001)

Components of the incident	Characteristics of inside perpetrator	Organizational response	Implications
Most practices required little technical sophistication	Unlike external perpetrators, rogue insiders are not technology savvy	Revise business rules of IT policy	Secure application access from a full range of users
Financial gain is the most important motivator	Most rogue insiders did not have a history of fraud or "hacking"[a]	Offset illegal financial gain by better salary and bonus	Although critical, financial gain is not the only motivation
Perpetrators conduct planned actions	Crimes are committed during daily job	Design and communicate incident response plan. Perform real time monitor for employees	Some perpetrations can be prevented at early stage
The demographics of perpetrators are heterogeneous	Insiders have diversified social backgrounds	Suspicious actions can be detected by various methods and people	Encourage reporting suspicious actions. Common perception may be inaccurate
Unauthorized access to applications	Most perpetrators exploited non-technical vulnerabilities such as over-the-shoulder and social engineering	Enforce internal security policy or invite external audit	Both technical/non-technical personnel must comply with corporate IT policy

Note: [a]Justifying the adoption of employee signature score

Table III.
Insider threats of Alibaba incident

management practices, whereas compromised insiders committed practices that required little professional knowledge and training. According to the work by Boss *et al.* (2009), employees tended to follow mandatory policies and security practices if they perceived themselves to be monitored in a controlled environment. Such a notion, along with the fact that most rogue insiders did not have a history of wrong-doings, leads to our suggestion of adopting signature models for employees inside Alibaba.

Discussions and conclusions

This paper represents a necessary step toward a more empirical data driven study. Further research can be done to explore the effectiveness of suggested strategies in a longitudinal or cross-sector setting. In this study, we have investigated a recent Alibaba B2B fraud incident, which has affected many buyers around the world and has resulted in over $6.6 million in losses. Our study provides value to the academic literature and practice by providing customizable policy suggestions, by re-evaluating the significant impact of internal fraud, and by offering effective measures that can be applied to other B2B service providers. We attempt to address the problem areas such as the member screening processes, internal controls, and collaboration with government agencies. Lessons learned from the incident yield practical advice about a company's pre-transaction activities. Companies should establish and enable a profile-based signature system for employees in addition to its members; cross reference the behavioral models of customers, member vendors, and employees; raise the admission standards of membership; keep close relationship with the vendors and continuously monitor vendors' statues, and strengthen the hiring process by establishing reference-based networks for sales representatives. About the post-transaction activities, the case of Alibaba illustrates that it is necessary to

conduct timely updates of account profiles for both employees and members. Cross references with updated blacklist databases are crucial countermeasures, which keep buyers informed at the same time.

Another contribution of this paper lies in its disclosure of a common yet often overlooked factor of Chinese online frauds – the customer acquirement strategy. Many fraudulent incidents that we have witnessed in Alibaba's case involved insider-vendor collaborations. As previously mentioned, the digital gaps among business practitioners may lead to under-the-table transactions, which should be prohibited by the electronic information systems. Today, most B2B providers enforce client-side signature authentication only. This paper, therefore, serves as educational materials to promote practitioner awareness of rigorous signature systems for both employees and clients.

Meanwhile, the one thing that stands out from the case is the cooperation between a company and the state government. Due to the nature and the size of the fraud ring, we believe that a call for government intervention is loud and clear. Fighting the black fraud ring markets cannot be accomplished by any individual company alone. Government interventions, sometimes even international organizations' interventions, are necessary to establish better legal systems to keep up with the ever-changing innovative internet crimes tactics. More effective law enforcement efforts to punish the offender and better information systems to keep legitimate companies timely informed about the fraudulent traders are in need. Fortunately, the Chinese Government is playing an increasingly important role in mitigating e-business deceptions. The digital law enforcement units were proven to be effective in Alibaba's investigation, and the Chinese Government is making commitments to start a database center to sort out legitimate companies.

In light of this, we suggest the following policy measures. First, a company should establish and actively maintain a network of employee references, and it should include background checks to the initial hiring processes. Doing so would allow firms to establish a tracking mechanism of employees' profiles and to enhance individual's perceptions of control. Second, firms should monitor employee behavior through objective and/or subjective measures. A signature model needs to be adopted to constantly monitor traders' behaviors and employees' actions. This is important because joint frauds between insiders and vendors are one of the most significant threats. Third, company policies need to spell out clearly the requirements of employees, such as being compliant with pre-incident planning and communications, providing continuous support for the internal threat management, and performing onsite tasks that require processing granularity. Lastly, a company should make a great effort to promote a better company culture and employee loyalty. Better employee training and clear expectations for ethical business conduct should be conveyed within the organization. Moreover, it has been indicated that higher education does not equate with higher ethical standards. Most of the criminals in Alibaba's case possess at least bachelor's degrees. Therefore, employee training must not overlook the importance of ethics education within the company.

References

ACFE (2010), *Association of Certified Fraud Examiners: Technical Report on Occupational Fraud and Abuse*.

Adepoju, A.S. and Alhassan, M.E. (2010), "Challenges of automated teller machine (ATM) usage and fraud occurrences in Nigeria – a case study of selected banks in Minna metropolis", *Journal of Internet Banking & Commerce*, Vol. 15 No. 2, pp. 72-80.

BBC News (2011), "China arrests 36 for fraud on Alibaba and other sites", July, available at: www.bbc.co.uk/news/business-13986308 (accessed December).

Boss, R.S., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Boss, R.W. (2009), "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security", *European Journal of Information Systems*, Vol. 18, pp. 151-64.

Business Week (2011), "Alibaba fraud scandal may help Google, Global Sources", February, available at: www.businessweek.com/news/2011-02-28/alibaba-fraud-scandal-may-help-google-global-sources.html (accessed December).

Cahill, M., Lambert, D., Pinheiro, J. and Sun, D. (2000), *Detecting Fraud in the Real World*, Technical Report, Bell Labs, Lucent Technologies, New York, NY.

Choo, K.R. (2011), "The cyber threat landscape: challenges and future research directions", *Computer & Security*, Vol. 30, pp. 719-31.

Choudhury, V. and Sabherwal, R. (2003), "Portfolios of control in outsourced software development projects", *Information Systems Research*, Vol. 14 No. 3, pp. 291-314.

Cortes, C. and Pregibon, D. (2001), "Signature-based methods for data streams", *Data Mining and Knowledge Discovery*, Vol. 5, pp. 167-82.

Dhillon, G. (2001), "Vilation of safeguards by trusted personnel and understanding related information security concerns", *Computer & Security*, Vol. 20 No. 2, pp. 165-72.

Edge, M.E. and Sampaio, P.R.F. (2009), "A survey of signature based methods for financial fraud detection", *Computer & Security*, Vol. 28, pp. 381-94.

Ferreira, P., Alves, R., Belo, O. and Cortesao, L. (2006), "Establishing fraud detection patterns based on signature", *Proceedings of Industrial Conference on Data Mining, Leipzig, Germany*, pp. 526-38.

Hu, Q., Hart, P. and Cooke, D. (2007), "The role of external and internal influences on information systems security – a neo-institutional perspective", *Journal of Strategic Information Systems*, Vol. 16 No. 2, pp. 153-72.

IC3 (2011), *IC3 Annual Internet Crime Report 2011*, pp. 10-11, Internet Crime Complaint Center, available at: www.ic3.gov/media/annualreport/2010_ic3report.pdf (accessed July 2011).

Kochetova-Kozloski, N., Messier, Jr, Willam, F. and Eilifsen, A. (2011), "Improving auditors' fraud judgments using a frequency response mode", *Contemporary Accounting Research*, Vol. 28 No. 3, pp. 837-58.

Laufer, D. and Betzer, S. (2010), "Teaching notes: hide and seek: a divorce fraud case study", *Journal of Forensic Studies in Accounting & Business*, Vol. 2 No. 1, pp. 67-72.

Lee, A. (1989), "A scientific methodology for MIS case studies", *MIS Quarterly*, Vol. 13 No. 1, pp. 33-50.

McGlasson, L. (2010), "Agencies issue ACH, wire fraud advisory", March, available at: www.govinfosecurity.com/articles.php?art_id¼2298 (accessed 17 December 2011).

Mieke, J., Nadine, L. and Koen, V. (2010), "Internal fraud risk reduction: results of a data mining case study", *International Journal of Accounting Information Systems*, Vol. 11, pp. 17-41.

Owhoso, V. and Weickgenannt, A. (2010), "Vinand Petroleum, Inc.: initial audit engagement and fraud risk case for a specialized industry", *Issues in Accounting Education*, Vol. 2 No. 2, pp. 331-46.

Reffett, A.B. (2010), "Can identifying and investigating fraud risks increase auditors' liability?", *Accounting Review*, Vol. 85 No. 6, pp. 2145-67.

Rotem, Y. (2011), "Company duplication – plain fraud or a 'poor man's' bankruptcy? A case study in the financial distress of small businesses", *International Insolvency Review*, Vol. 20 No. 2, pp. 131-59.

RSA (2010), *RSA Online Fraud Report*, pp. 1-2.

Sadan, Z. and Schwartz, D. (2010), "White script: using social network analysis parameters to balance browser usability and malware exposure", *Computer & Security*, Vol. 30 No. 1, pp. 4-12.

Short, J., Williams, E. and Christie, B. (1976), *The Social Psychology of Telecommunication*, Wiley, New York, NY.

Tomasic, R. (2011), "The financial crisis and the haphazard pursuit of financial crime", *Journal of Financial Crime*, Vol. 18 No. 1, pp. 7-31.

Viaene, S., Dedene, G. and Derrig, R.A. (2005), "Auto claim fraud detection using Bayesian learning neural networks", *Expert Systems with Applications*, Vol. 29, pp. 653-66.

Wall Street Journal (2011), "Alibaba.com CEO resigns in wake of fraud by sellers", *Wall Street Journal*, available at: http://online.wsj.com/article/SB10001424052748704476604576157771196658468.html#ixzz1i4jOvBAF (accessed July).

Xiao, B. and Benbasat, I. (2011), "Product-related deception in e-commerce: a theoretical perspective", *MIS Quarterly*, Vol. 35 No. 1, pp. 169-95.

Further reading

Alibaba News (2011), *Alibaba Group*, June, available at: http://news.alibaba.com/specials/aboutalibaba/aligroup/index.html (accessed August).

About the authors

Chengqi (Chen) Guo is an Assistant Professor of Computer Information Systems & Management Science in the College of Business at James Madison University, where he became a member of the Madison Research Fellows. He received his PhD degree in Business Information Systems from Mississippi State University, USA. He received a Master's of Operations Management & Information Systems (OMIS) from Northern Illinois University (USA) and a BS in International Marketing from Guangdong University of Foreign Studies (GDUFS), China. He is currently working as a Senior Consultant for JDArray Co. Ltd His research interests are social media, mobile computing (commerce, technical innovation, and social networking service), human computer interaction (adoption, trust, privacy, and communication), cross-cultural studies, and information systems security. Chengqi (Chen) Guo is the corresponding author and can be contacted at: guocx@jmu.edu

Xiaorui Hu is an Associate Professor of Decision Sciences and Information Technology Management at the John Cook School of Business, Saint Louis University. She received her PhD in Economics from the University of Texas at Austin. Her research focuses on trust related issues in electronic commerce, culture impact on international business, and information security. She has published in *Information Systems Research*, *Decision Support Systems*, *IEEE Computer*, *Journal of Organizational Computing and Electronic Commerce*, and other academic journals.