

**ONLINE | PAYPERS**

## Online fraud: a never-ending battle

FFIEC issues supplement to guidance on internet banking authentication	1
Exclusive interview: Timothy Eades, CEO of Silver Tail Systems	2
Expert opinions	3
Teenagers easily fall victims to online fraud, parents should know the risks	6

**Online fraud: a never-ending battle****FFIEC issues supplement to guidance on internet banking authentication**

The Federal Financial Institutions Examination Council (FFIEC) has issued a supplement to its guidance, called the Authentication in an Internet Banking Environment, released in October 2005. The supplement is set to reinforce the risk-management framework approached in the initial guidance and update the FFIEC member agencies' supervisory expectations with regard to customer authentication, layered security and other controls in the online environment.

The supplement stipulates new rules for online security according to which banks should focus on layered security and fraud monitoring to better protect against cybercrime. According to the FFIEC, a layered security program includes:

- fraud detection and monitoring systems that include consideration of customer history and behaviour and enable a timely and effective institution response;
- the use of dual customer authorization through different access devices;
- the use of out-of-band verification for transactions;
- the use of dual customer authorization through different access devices;
- the use of out-of-band verification for transactions;
- the use of "positive pay," debit blocks [Read more](#)

**Citigroup credit card customers lose USD 2.7 million in security breach**

Following the cyber-attack against Citigroup credit card portal in May 2011, nearly 3,400 Citigroup credit card customers have suffered a loss of USD 2.7 million, online media outlet buy.wsj.com reports. [Read more](#)

**Ping Identity secures USD 21 million in funding round**

US-based internet identity security services provider Ping Identity has secured USD 21 million in funding round from a group of investors. The new funding will enable Ping Identity to invest in its next generation of cloud identity management services and global sales. [Read more](#)

**First National Bank of Pennsylvania selects Memento to combat deposit account fraud**

US financial services provider First National Bank of Pennsylvania has entered a partnership with Memento, a fraud management services provider for banks, to combat deposit account fraud over multiple payment types and delivery channels. [Read more](#)

**EXCLUSIVE INTERVIEW**

with  
Silver Tail Systems

Why Silver Tail Systems? Because you need every advantage.

- exclusive interview with Timothy Eades , CEO of Silver Tail Systems -



With over 17 years of leadership experience in sales, marketing, and general management, Timothy has deep expertise in driving high growth for computing, security and enterprise software companies. His business experience includes providing technology solutions to Fortune 100 companies, large enterprises, mid-size businesses, as well as consumer markets. Timothy holds advanced degrees in business, international marketing, and financial analysis, primarily from Solent University in England.

**What is Silver Tail Systems' role in the prevention of online fraud and identity theft?**

Authentication systems can provide only limited protection against attacks on web sites; where they fail – for example when the criminal is using the victim's computer – it is only through the use of web session behaviour analytics, which is how anomalous behaviour is exposed, that you can detect attacks like Man in the Browser. This is what Silver Tail's products do.

In addition, we can detect some of the pre-cursors to fraud. Criminals often visit their target website beforehand to gather information required for their attack. These activities can be perpetrated through a web site and we are able to detect them as they are happening – before the fraud takes place.

**What makes the company's product offering different from other similar ones available on the market?**

Where other fraud prevention products look deep at individual transactions – like signing or transferring money out of an account – our products monitor the entire web session and can identify when there is abnormal behaviour.

This goes way beyond authentication and gives web site owners the ability to react dramatically faster than if they were using more traditional tools; our products can be configured in real time to deflect threats as they emerge; this is a unique capability.

**In your opinion, what are the most common indicators of a fraudulent transaction?**

The most common indicator is that the web session looks different from what is normal for the population of the website. Legitimate customers don't steal data or money or try to infiltrate your systems. Criminals' behaviour looks different because their end goal is different.

**Is it fair to think that in fighting online fraud there is a 'one-size-fits-all' strategy? What is your company's approach in this respect (have you developed specific products for specific industries or regions) and what is your main target market?**

Fighting online fraud is not one-size-fits-all. Because people use websites in different ways, depending on the type of the site, their behaviours will be different. Our algorithms automatically determine the normal behaviour for the site – independent of what type of site it is.

“It's encouraging that the market is starting to understand the nature and breadth of attacks that are currently being perpetrated.”

**Timothy Eades , CEO of Silver Tail Systems**

**As far as the adoption of online fraud prevention measures/sophisticated security systems is concerned, where do you think the main challenges come from?**

There seems to be a growing understanding that the attacks against websites are not just against the money transfer part of the site. If you look at the recent attacks that have impacted some of the big brands, many did not directly target monetary transactions.

It's encouraging that the market is starting to understand the nature and breadth of attacks that are currently being perpetrated; by knowing more about the threat companies can make informed decisions about how to respond and which tools they need to mitigate negative impacts.

**Which are some top directions of development for your company?**

Silver Tail's mission remains totally focused upon detecting and mitigating the impacts of fraud directed towards web sites (such fraud is now commonly called cybercrime); with the recent VC funding injection that mission will be strengthened and deepened by increasing investment in research, product development and customer support.

Most critically Silver Tail will extend its geographic reach, bringing to European Banks, on-line Retailers and Government agencies our complete solution that protects web sites from both known and modern - day emerging threats; this expansion into Europe will include providing first - line product support.

### Background on Silver Tail Systems

Silver Tail Systems is the leading provider of predictive analytics for detection and prevention of fraud and abuse to some of the leading websites in the world. The company offers the industry's most comprehensive suite of fraud detection and mitigation solutions.

Serving some of the world's largest financial institutions and e-commerce companies, Silver Tail Systems' award-winning solutions are made possible by the unmatched

expertise of its management and technology teams, who bring deep experience, know-how and personal commitment to protect their customers' businesses against online fraud.

### EXPERT OPINIONS

## ThreatMetrix™

### Stolen Identity Fraud: It's Not About Just Chargebacks Anymore

**- By Reed Taussig, CEO and President, ThreatMetrix—**

“There is no doubt that online credit, debit, and more recently gift card and alternative payment fraud, continues to be a significant factor affecting the confidence of consumers and the profits of online merchants. However, the losses associated with fraudulent payments potentially pales in comparison to the costs associated with stolen identities. The recent breaches suffered by Sega, Sony, Citibank and others clearly shows that fraudsters are not only after credit cards but also the personally identifiable information (PII) that can enable them to steal a person's identity which is often far more valuable than just a stolen credit card. Using stolen identities, fraudsters are able to access personal bank and brokerage accounts, fraudulently apply for loans or new credit cards and in some cases completely ruin a person's credit score.

Historically, the vast majority of retailers have only concerned themselves with trying to stop the use of stolen credit cards in order to control chargebacks and reduce the loss of cost of goods sold. Almost none of the more than 500 retailers using the ThreatMetrix™ Cloud-Based Fraud Prevention Platform solution apply anti-fraud measures to protect customer log ins or new account originations. In most cases the credit card number a consumer has stored on a retailer's site is not accessible. However, the name, address,

email address and telephone number of that consumer is accessible and with this information in hand, fraudsters will try to compromise a person's bank account or use that information to fraudulently apply for credit or other services. The consequences can be and in most cases are significant.

Retailers engaged in e-commerce now need to employ the very effective anti-fraud tools that they are using to stop payment fraud to every consumer access point on their Web sites in order to protect themselves from the horrific costs associated with the loss of personally identifiable information. In the case of the Sony PlayStation breach no credit cards were stolen. Nevertheless, Sony's cost to recover from that breach is estimated to be more than \$170 million. It isn't just about chargebacks anymore."

Reed Taussig has more than 30 years of experience in the computer hardware and software fields. Prior to ThreatMetrix, Mr. Taussig was president and CEO of Vormetric, Inc., a leader in data privacy and protection. Under his leadership, Vormetric established itself as a leading provider of encryption solutions for the Payment Card Industry Data Security Standards industry.

Mr. Taussig also served as president and CEO of Callidus Software (NASDAQ: CALD), the leading provider of enterprise incentive compensation management application systems. As founding CEO and the fifth employee, Mr. Taussig led the growth of company to more than \$70 million in revenues and over 350 employees. Mr. Taussig holds a bachelor's of arts degree in economics from the University of Arizona.



**Reed Taussig, CEO and President, ThreatMetrix**

## SIX CARD SOLUTIONS

### Keeping cyber criminals out

- By Sascha Breite, Head of the e-commerce competence centre at SIX Card Solutions -

"Online fraud is firmly back in the spotlight after hackers stole the personal details, including credit card information, of millions of Sony PlayStation customers recently. There has been much in the news about the potential impact this fraud could have on consumers but online businesses are just as vulnerable to being targeted by fraudsters.

For example, a criminal with thousands of stolen credit card details at their disposal, firstly needs to find out which ones can be used for genuine online payments. The typical way in which they do this is by placing fake orders through a merchant's website to find out which cards are enrolled to 3-D Secure and thus require a password to verify a payment. While businesses can block the fake orders and IP addresses, the result is that online stores become a "credit card screening tool" for criminals, making the merchant shop effectively an instrument of the fraud.

Another issue that online merchants often face in terms of fraud is when they look to expand internationally. While "Verified by Visa" and "MasterCard SecureCode" are powerful tools in the fight against fraud, not all card issuing banks have enrolled their card holders to 3-D Secure.

As a result, a merchant that is growing cross-border can often come up against customers who are unfamiliar with 3-D Secure, for example in France, who can be deterred from completing a purchase due to this unknown feature. To increase the order rate in these countries, merchants are beginning to disable 3-D Secure on their websites but this is obviously increasing their exposure to fraud and thus their charge back rates.

As well as being the target for fraudulent transactions, online merchants also have to, like Sony, ensure their customers' card details are stored and protected correctly so they do not fall into fraudsters' hands. The launch of the PCI programme has been a successful initiative in forcing merchants to look at their IT infrastructure and processes and make sure their card payments processing is secure.

Specifically, merchants with a high volume of transactions are increasingly becoming aware of the risks associated with handling credit card data and the potential fraud losses which can arise if card data is stolen from their systems. However, there are still some SME merchants who do not have a complete overview of their credit card processing and continue to store card details on their systems without them being encrypted. This can result in security holes which intruders or employees can exploit for criminal purposes.

In light of this myriad of issues, it is clear that online merchants need to have appropriate tools and risk management applications in place to not only better protect themselves from fraud but to ensure their sites are not misused to aid fraudsters. Coupled with this, merchants need to be able to keep costs down and business fluid so achieving a fine balance between higher revenue and fewer charge backs is key. Only then, will businesses be able to keep the cyber criminals at bay.

Sascha Breite is Head of the e-commerce competence centre and Managing Director of SIX Card Solutions Germany. As part of his role, he manages the business around the virtual payment solutions, which includes distance payment services for e- and m-commerce as well as integrated payment solutions for the POS.

**Sascha Breite, Head of the e-commerce competence centre at SIX  
Card Solutions**



## Online retailers, if the only risk you are worried about is fraud, think again

**- By Danny Chazonoff, President of Optimal Payments' NETBANX division -**

“ Much of the recent discussion in online retail has been around fraud prevention. Of the three major areas facing e-tailers, this is actually the least important because it is the most discretionary.

When you sell online, you have to capture who your customers are, where to ship, and take payment all electronically. And you want to retain that information so they can easily purchase again. In doing this you face three very different areas of risk.

1 – What you have to do. As a commercial consumer-facing business you are required to comply with certain standards. The most significant obligation is PCI DSS compliance, designed to protect credit and debit card information. If you are not currently compliant or your payment provider is not PCI level 1 certified, then you need to fix this. Fines can be up to USD 25,000 a month.

2 – What your customers expect. You are expected to take care of the personal consumer information you hold and there are heavy costs associated with data breaches, typically running at \$268 per lost customer record according to analysts. Sony's breach could cost them USD 20 billion. You should do your own calculation based on your customers.

The more advanced payment providers offer implementation via a secure hosted checkout page and then store all your customer name, contact and payment information on their hardened servers, not yours. They provide a “token” for each customer, which allows

repeated single-click checkout and rebilling without you ever needing to hold that information. Security may not be your business, but it is theirs, so pick wisely, then keep your implementations up to date using your payment provider's latest approaches.

3 – What you would like to do. Online fraud happens in seconds and can cost businesses up to 10% of gross revenues. Most payment providers offer 3-D Secure™ and the basic card checking tools. The smart ones embed full anti-fraud suites into their services. These have real-time rules that sniff and snuff out fraud before it happens. Any experienced provider should be able to guide you with the right rules for your industry.

Because you can reach new customers in their homes at times they want, there are huge opportunities to be made online. Fraud losses may be top of mind, but first you need to protect your business by doing the things you need and are expected to do. Smart retailers are well aware of this and leverage their payment partners to maintain their success.

Danny Chazonoff was appointed President of Optimal Payments' STP business on 1 February 2011 following the acquisition of the business of Optimal Payments (Optimal) by NEOVIA Financial (now renamed Optimal Payments). Danny served as Optimal's Chief Operating Officer and Chief Technology Officer since November 2006. He has held a number of roles including CTO and COO with Optimal since its formation in 1999 as SureFire Commerce (renamed Terra Payments) and also at BCE Emergis. He brings a wealth of international payments expertise and IT experience to the STP business of Optimal Payments business.



**Danny Chazonoff, President of Optimal Payments' NETBANX division**

## FOCUS ON REPORT

### **Teenagers easily fall victims to online fraud, parents should know the risks**

Teenagers are particularly vulnerable to scammers because they spend so much time online. They are willing to share their personal data with strangers online either when they are shopping or engage in social networking websites. Their behaviour online should be constantly monitored by parents who should be aware of the online threats and teach their children how to avoid them.

In the US, 11 percent of teenagers prefer to make purchases online, according to a study released by the investment banking firm Piper Jaffray. The research has also indicated that the lack of access to payment methods such as credit cards is one of the factors that prevent teenagers from buying online.

Such findings, along with the growing number of teenagers shopping online (especially those under 18 who are not eligible for credit cards) and the online security-related issues deriving from the process have determined payment services providers and technology companies to develop payment systems specifically tailored for this target group.

### **Payment methods available for teenagers**

Companies involved in the payments industry have designed various payment methods for teenagers to enable them to make online purchases and to allow parents to control their online expenses in order to avoid cyber fraudsters' attacks.

For example, BillMyParents is a youth payment system which enables teenagers to shop online without a credit card, while giving parents the ability to track and control spending. By clicking on BillMyParents button at the online merchant's checkout, teenagers send a request to their parents or other relatives on a potential purchase by email or SMS

through an automated system, which includes details on the price of the item, the store that is selling it and a personal note written by the child as a sort of justification for why he needs the product. Parents have to go through a registration process and mention the name of the child who will shop on the website.

Another payment system for teenagers, dubbed Virtual Piggy, was created by US-based developer of platform technology Moggle. The platform enables children to transact with online merchants, games and social networks under parents supervision. The Virtual Piggy technology allows parents to set up an online spending profile and control their children's spending on the web.

Other similar payment systems include the Visa-branded prepaid card for teenagers buying online powered by the Australian financial services provider ANZ Bank and the PayPal's Student Account program which enables young users to use a PayPal-branded MasterCard debit card that is connected to a parent's PayPal account.

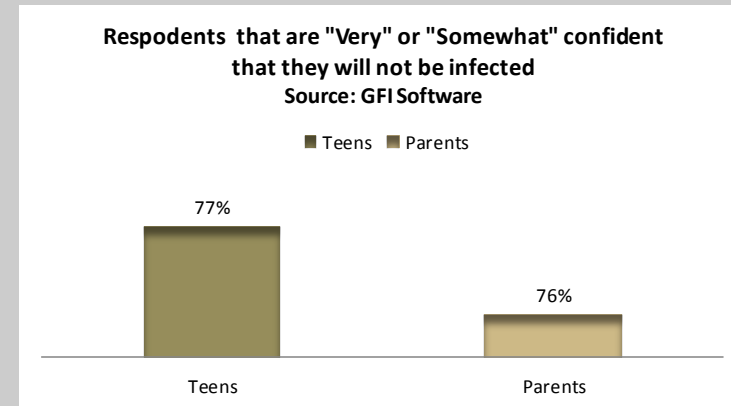
**Despite high confidence in not being infected by viruses, teenagers still fall victims to malware infection**

Parents have a very difficult job when protecting teenagers from online threats, due to the growing ubiquity of internet access. Nowadays, teenagers are able to access the internet from home, school, mobile phones and friends' houses. Both parents and children should be aware of the risky behaviour on the internet which could threaten their sensitive data integrity.

When it comes to malware infection, although 76 percent of parents and 77 percent of teenagers in the US are either very or somewhat confident they will not be infected by viruses, a large percentage is still being infected, a recent survey has unveiled.

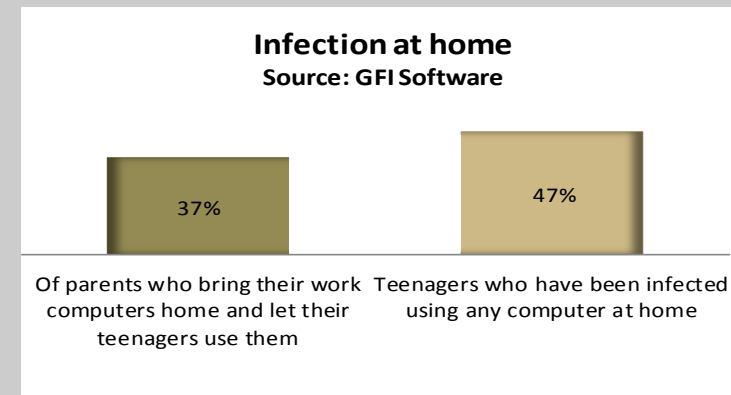
According to the Parent-Teen Internet Safety Report 2011 released by the US IT services provider GFI Software, nearly 47 percent of the teenagers have been infected by a virus

while using a computer at home giving cyber killers the opportunity to steal the personal identification information of both teenagers and parents which can result in financial loss.



The study indicates that nearly two-thirds (65 percent) of the parents involved in the survey have had their home computer infected by a virus. 55 percent of these parents have been infected by a virus more than once. Almost two-thirds (62 percent) of those who have been infected consider the problem to be somewhat or very serious.

Furthermore, the study points out that 37 percent of parents who bring their work computer at home allow their teenagers to use it. Moreover, 90 percent of the interviewed parents use their work computers at home for personal business.



In terms of security measures, the study reveals that 89 percent of parents have antivirus software installed on their computers. Of these, 28 percent update their virus definitions daily, while 24 percent are not sure if they are updating these definitions at all.

#### Teenagers, victims of online bullying

According to the study, when it comes to online teen communication which could result in sensitive data disclosure, 11 percent of teenagers have reported having been bullied online. 31 percent of teenagers admit that they have communicated something to someone online or via text message that they would not feel comfortable saying to them in person.

More than half of parents and teenagers involved in the study own a Facebook account. Of these, 87 percent are friends with one another on the website. 83 percent of teenagers with Facebook accounts have indicated that they know how to use privacy settings so they can hide content from their parents. 34 percent of the polled teenagers have created an online Facebook account which their parents do not know about.

Of the surveyed teenagers, 29 percent have been contacted online by an unknown person. Of this group, 62 percent have been contacted by a stranger on more than one occasion while 23 percent claim they have responded to the stranger in some way.

In conclusion, parents face a real challenge when it comes to controlling teenagers online who can easily fall victims to cyber-attacks, malware, inappropriate content and predatory behaviour from both known and unknown people.

On the other hand, both parents and children should understand that risky behaviour on the internet may result in problems ranging from data theft to financial losses.



## Complex threats require comprehensive solutions

- By Jeff Liesendahl, CEO of Accertify -

“To keep pace with the needs and desires of an increasingly tech-savvy customer, today’s e-commerce businesses are expanding the number and complexity of payment channels they offer and methods of payment they accept. As we know from the steady stream of news reports on security breaches, fraudulent individuals are concurrently continuing to develop their own sophisticated skills in order to exploit this new technology. As a result, it is more important than ever for companies to have holistic and enterprise-wide fraud detection and resolution systems that can address all of these channels in whatever form the transaction data takes.

Complex threats require comprehensive solutions. In order to ensure the security of payer information and prevent becoming the victim of payment fraud, companies today need to employ fraud detection services that use all transaction data – regardless of source – to monitor all their payment channels across all payment methods. This means monitoring beyond the web and point of sale, to also cover mobile, kiosk and call center payments. And a good fraud prevention provider should support the full array of payment methods available to today’s customer, including credit and debit cards, ACH, e-wallet and other online services.

The best solutions are customized fraud screening rules tailored to your business that are nevertheless cost-effective, easy-to-use and flexible enough to adapt to evolving threats to your business and manage the full lifecycle of fraud from detection to resolution. This total solution will not only help protect your profit margin, but it also will ensure that customers trust your ability to safeguard their information and are willing to do business with you in the future.

Jeff Liesendahl is the CEO of Accertify, a leading provider of hosted software solutions and tools and strategies for preventing fraud and mitigating enterprise-wide risks. Accertify's Interceptas platform delivers unparalleled flexibility in combating various types of criminal behavior, including fraud related to card-not-present purchases, online scams and policy abuse, merchandise returns and exchanges and other data management challenges.



Jeff Liesendahl, CEO of Accertify

## NEWS

### SecurEnvoy rolls out two-factor authentication token application

SecurEnvoy, a provider of tokenless two-factor authentication services, has launched a new version of its two-factor authentication token application, online media outlet rpfconnect.com reports. [Read more](#)

### Garanti Bank upgrades fraud protection service via FICO Falcon Fraud Manager

Turkey-based financial institution Garanti Bank is set to upgrade protection for all its cards products, consumer loans, credit card applications and current account / DDA transactions via FICO Falcon Fraud Manager 6 powered by global decision management services provider FICO. [Read more](#)



### UK: Mobile, social media commerce to increase online fraud to GBP 195.3 million by 2015

Driven by mobile and social media shopping, online fraud in the UK is expected to witness an 18 percent growth, from GBP 165.2 million in 2011 to GBP 195.3 million in 2015, a recent survey has revealed.

According to a report conducted by the Centre for Economic and Business Research (Cebr) on behalf of UK online payment services provider PayPoint.net, the growth of mobile and social media commerce is expected to drive total online sales of GBP 33.7 billion by 2015, recording an annual growth of 4.5 percent. [Read more](#)



**About:** Online Paypers is a bi-weekly update on developments in online payments by The Paypers, the portal for payment professionals.

**Editors:** Adriana Screpnic, Monica Gaza, Daniela Vicovan, Mihaela Mihaila and Melisande Mual.

**Website:** For more information, please visit our websites: [www.thepaypers.com](http://www.thepaypers.com)

**Contact:** For more information, you can contact us at: [info@thepaypers.com](mailto:info@thepaypers.com)

**Subscription info:** Online Paypers is a product of The Paypers and is published 24 times per year. Year subscription price: €495

**Copyright:** 2011 © The Paypers. All rights reserved. Reproduction or redistribution in any form without explicit prior written permission of The Paypers is prohibited.