How New Device Technology is Shifting Payments Authentication: Why Multi-Layered Authentication is Critical Now

The past two years have demonstrated the need for comprehensive and streamlined authentication at every level in every channel. In a given year, 25% of companies are impacted by data breaches[1] – a scary statistic that has been highlighted with the mega retail breaches of 2013 and 2014. Ponemon Institute reports that the average annualized cost of cyber crime is $12.7 million per organization every year (based on a benchmark study of 257 organizations). The threats merchants face run the gamut – from denial-of-service attacks, malicious insiders and web-based attacks (all of which account for over 55% of total cyber crime costs) to account takeover and other emerging vulnerabilities. With a 45-day average to contain these types of attacks, they're a serious threat to merchants' payment processing.[2] Despite the gravity of these statistics, only about 2% of tech budgets are spent on security.[3]

Only about 2% of tech budgets are spent on security.[3]

The "Good News/Bad News" Outlook of CNP & Omni-Channel Commerce

Card-Not-Present (CNP) commerce is steadily growing, with global retail e-commerce projected to hit $2 trillion by 2016.[4] This growth is bolstered by the increasing adoption of smartphones, as almost a quarter of people worldwide own a smartphone.[5] Online sales rose 15.4% last year over 2013, totaling $304.91 billion.[6] That's the good news for merchants who are omni-ready, however, it also points to increased opportunities for fraudsters to feast on the profits of unsuspecting and unprepared merchants. Now the bad news. Fraud does not play favorites and the economic impact of fraud weighs heavily on merchants of all sizes. Companies with 100 employees or less average $154,000 annually to fraud, according to the Association of Certified Fraud Examiners (ACFE).[7] Overall, merchants lose $3.08 per dollar of fraud incurred.[8] Mobile elevates that cost even more, with fraud in this channel costing merchants $3.34 on the dollar.[9]

Mobile and the Device-Driven Purchase

Mobile's convenience has it poised as an up-and-coming favorite payment method. Mobile payments accounted for $52 billion in transactions in the U.S. in 2014, should hit $67 billion this year and could skyrocket to $142 billion by 2019.[10] As e-wallets and mobile proximity payments gain traction, the fraudsters continue to seek out vulnerabilities and opportunities to seize valuable data. Recent reports have shown that on average, companies lose $92.3 million every year to mobile fraud, **with some companies losing 25% of their revenues to mobile fraud.**[11]

With the Internet of Things (IoT) picking up momentum in the payments space, devices will continue to be a consideration for payment methods, despite the fact that there are many vulnerabilities that haven't been addressed. Companies have already begun developing payment-enabled digital signage, kiosks and intelligent vending machines, making payments possible through common things.[12] Mobile payment acceptance will merge with point-of-sale technology to enable consumers to shop through a variety of physical objects, but mainstream success will require advanced security. A recent study on IoT showed the following:

- 90% of devices collect at least one piece of personal information through the device itself, a mobile application or via the cloud[13]
- 80% of devices (in conjunction with their mobile app and cloud components) do not require adequate passwords[14]
- 70% of devices (in conjunction with their mobile app and cloud components) let attackers use account enumeration to identify valid user accounts[15]

Since many devices use unencrypted network services, there are gaping vulnerabilities that open up opportunities for attackers to gather valuable, sensitive data like name, date of birth, address, and in some cases, credit card numbers.[16] In short, devices open up a world of hurt for merchants who don't take appropriate steps to secure omni-channel transactions from end-to-end.

Current and Emerging Omni-Channel Fraud Prevention Tools

Passwords are easily hacked, especially when 63% of consumers use one password for all online accounts.[17] The slew of data breaches illustrates that this single-factor authentication method is becoming much less useful as a security mechanism. That said, companies that use a multi-layered, multi-channel authentication approach to security and risk mitigation make it exceedingly difficult for fraudsters to prevail. As the EMV migration swings into full-effect, the chip & PIN technology will help alleviate lost/stolen fraud and bolster authentication beyond a static password. There are a number of current and emerging tools that – when proportionately layered and tailored to a business – can effectively prevent fraud:

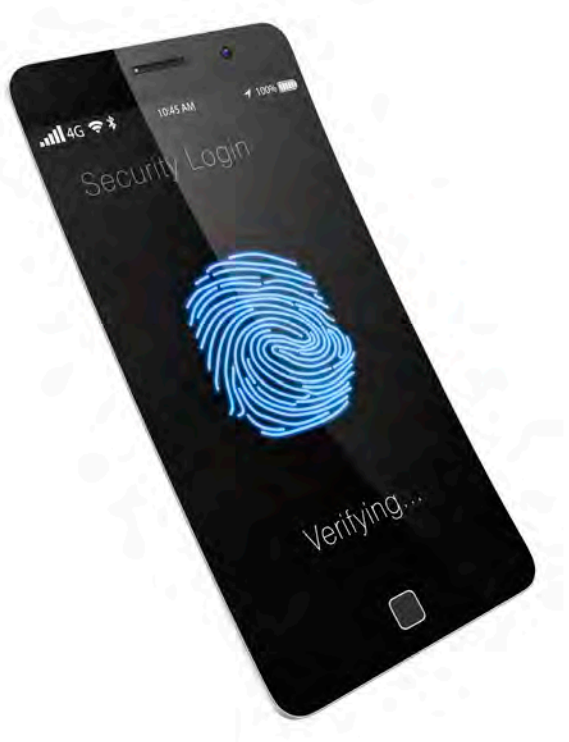
3D SECURE – Enhanced 3DS has shifted from static password authentication to dynamic authentication, rendering it more user-friendly and difficult for fraudsters to hack.[18] Additionally, merchants can choose the transactions on which they use 3DS, through a rules engine.[19] Many issuers are now using risk-based authentication, using data from the Access Control Server to assess the risk of each transaction and requiring specific authentication measures for high-risk transactions.[20]

PATTERN-BASED INTELLIGENCE – Using transaction authentication and pattern-based intelligence provides an additional security layer for high-risk transactions. This may include a number of elements like Out-of-Band (OOB) transaction verification, behavioral analysis and transaction monitoring.[21]

DEVICE AUTHENTICATION – This tool is used to verify that the person attempting to make a purchase is using a known device. These solutions often combine device ID technology with geolocation and proxy detection.[22]

APPLICATION SECURITY – This security layer increases the difficulty for hackers by protecting sensitive information delivered via apps on mobile devices through mutual authentication.[23]

BIOMETRICS – This technology is becoming mainstream and is commonly seen in Apple Pay's Touch ID feature. The addition of biometrics (three-factor authentication) can ensure and protect the identity of the cardholder because the identifiers are unique to the customer and they are easily accessible for the user.



What is Multi-Layered Authentication?

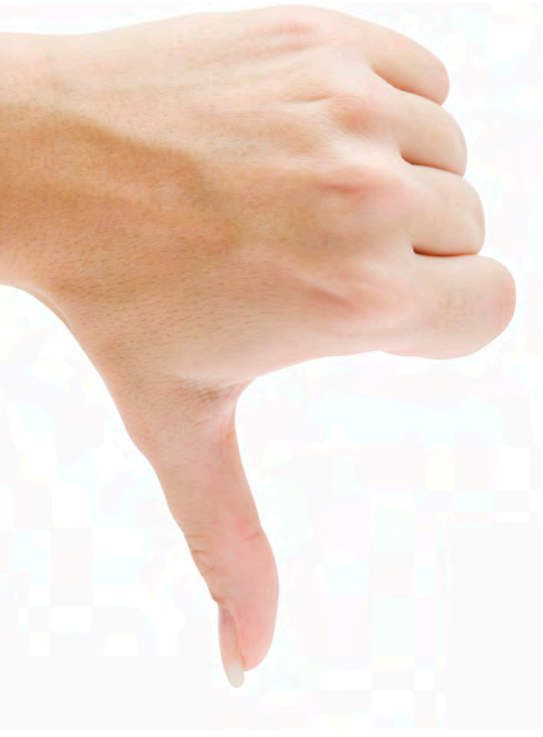
Multi-layered authentication adds layers of security without adding friction for loyal customers. Layering tools such as digital fingerprinting with biometrics helps merchants identify risks along every step of the transaction lifecycle without reducing the quality of the user experience. By covering all touch points with different authentication methods, merchants can ensure that payments are protected from end to end.

TOUCHPOINT	SECURITY FEATURE	WHAT IT DOES
ACCOUNT CREATION – this touch point is where the user registers or sets up an account. This is the first opportunity an organization has to validate that the person attempting to register is who they say they are. This prevents unauthorized users from attempting to login from a person's account in the future.	Text to phone	This method allows a merchant to associate a device with a registered user and his/her account.
	IP address	Merchants can log the IP address of the machine or device used to create an account and use that IP address to validate a person's identity in the future, since IP address is unique to each device.
	CAPTCHA	Captchas prevent automatic logins from bots or computers, though this security method has a 3% conversion rate loss.[24]
LOGIN – Once a user creates an account, the next touch point is when they actually log in to the account.	USB fobs	USB fobs with an LCD screen generate one-time use passwords. The user presses a button on the fob and a numeric code is generated and displayed for 30 seconds, which the user must enter into the application or site they are trying to access.[25]
	Security questions	This is not a desirable form of authentication as they can be easily hacked. The level of security is equal to that of a static password.
PURCHASE – the final touch point is when the user actually attempts a purchase through their account.	AVS	This authentication method verifies an account holder's billing address with the credit card issuer. AVS compares the address information that the cardholder provides with the information on file with the Issuer and sends a result code to the merchant indicating if the address is a match or not.[26]
	CVV2	This security feature is a popular tool for CNP authentication as it requires the user to enter the 3-digit CVV2 code found on the back of a credit card, verifying that the person attempting to make a purchase has the physical card in their possession.[27]
DEVICE-SPECIFIC - these tools and methods are meant to validate a cardholder through the device they're using.	Device fingerprinting	This method tracks characteristics (software versions, screen size, available fonts) associated with a specific device to create a unique profile of that device.[28]
	Checking for jail broken mobile devices	This allows merchants to detect jail broken devices, which can pose a threat since the security checks may have been removed in the smartphone operating systems through malware or other nefarious means.[29]
	Suspicious behavior and anomaly detection	This proactive measure is more secure than just requiring a signature. By using predictive analytics and advanced detection technologies, merchants can find behavior anomalies that may direct to compromised machines.[30]
	Identifying potential fraudsters using identity-masking tools	There are several sites that help browsers mask identifying characteristics and also tools available to discover fraudsters who are using this technology.[31]

Why Multi-layered Authentication is Critical

Multi-layered authentication is an essential component of any fraud and risk mitigation strategy, particularly as it relates to omni-channel and devices. In general, multi-layered authentication broadens the scope of verification and adds a layer of security without interfering with the customer experience. A streamlined, secure purchase experience requires merchants to balance different types of authentication with the costs of consumer friction. No one solution provides a "silver bullet" and merchants must weigh the pros and cons of fraud risk, customer experience and the total cost of the fraud prevention tools being used. Authentication for the device is no different; more consumers are using mobile and other devices to make purchases and merchants should adhere to the same security standards for these omni-channel purchases with an extra consideration for the user experience on each device.

Too little security can weaken brand reputation and can even make consumers leery about shopping with a merchant. Trust seals and security messaging throughout a merchant's website and the checkout process can be beneficial, as can Mobile-specific messaging.[32] Too much security is annoying to consumers and contributes to an already-high card abandonment rate – the average is 68.53%.[33] By asking for too much personal information upfront or preventing customers from logging on with new devices, merchants may be driving away legitimate sales.



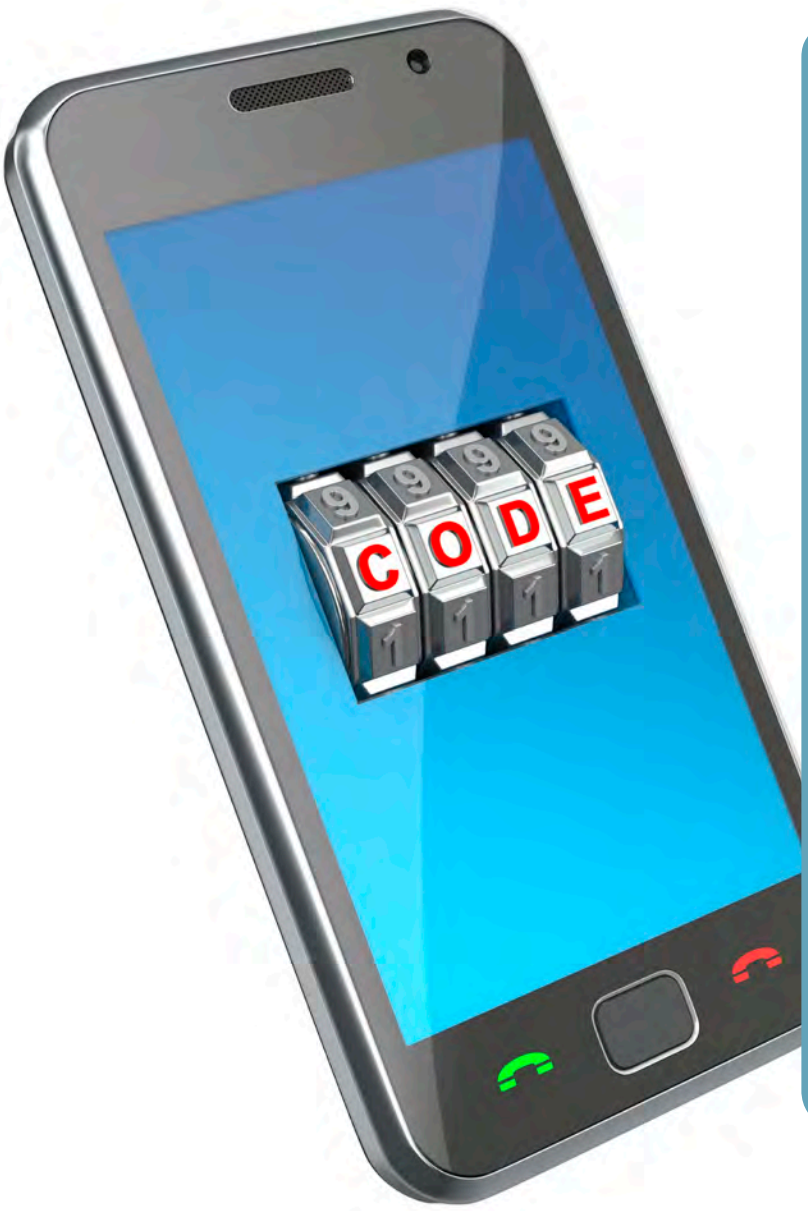
eCommerce merchants decline roughly 2.6% of all orders[34]

False Positives

False positives – legitimate, but declined orders due to too-sensitive fraud screening tools – are another thorn in the side of merchants. eCommerce merchants decline roughly 2.6% of all orders[34] – a potentially large chunk of revenue, though many merchants don't view it that way. By looking at declined orders as a cost avoidance rather than lost revenue, merchants are doing their business – and their bottom line – a disservice. Data shows that merchants' view on false positives is skewed – most merchants guess that they have a 10% false positive rate, that is, they decline roughly 10% of orders that should have gone through. Yet data shows that anywhere from 40%-75% of declined orders can be false positive declines[35], meaning merchants may be turning away a larger portion of legitimate orders than they think. When fraud controls are too conservative, merchants stand to lose a significant amount of potential income.

Too Much or Too Little - It's A Balancing Act

Merchants need to balance pre-sale screening tools with post-transaction measures to provide a consistent, safe and streamlined consumer experience. Merchants should adapt a proactive approach to fraud prevention rather than a reactive one that will inhibit sales through overreaching fraud controls. This is especially true for omni-channel where cart abandonment rates can reach a startling 97%![36] Post-transaction, chargeback notifications can boost fraud prevention awareness by acting as a feedback loop to compliment front-end fraud tools. This real time, notifications enable merchants to prevent disputes before they become chargebacks without negatively impacting sales. This also gives merchants an opportunity to fine-tune front-end fraud controls without worrying about the implications to fraud on the back-end.



Multi-Factor Authentication Technologies

One-Time Passwords (OTP): stores a shared seed or secret on an authentication device that generates a one-time passcode based on the token's secret to ensure authentication.[37]

Certificate-based Authentication (CBA): combines a public and private encryption key unique to each device. This may be done via USB tokens or smart cards.[38]

Context-based Authentication: works best in combination with other strong authentication techniques since it relies on contextual information to determine the authenticity of a user's identity.[39]

Best Practices for Device Authentication

70% of businesses conduct daily reconciliation of transactions[40] – a task that comes with great cost when you consider the significant amount of research that takes place on the merchant's part to follow up on questionable activity both internally and with the issuer. Today, it's even more important for merchants to have a strong authentication strategy to confirm user identities and the devices that are accessing otherwise secure networks. A successful strategy will entail a flexible approach that matches solutions to a merchant's business needs, unique users and risk profile. This often means combining authentication methods appropriately to risk levels for efficiency and cost-effectiveness.

Gartner notes that the best approach to authentication is "risk-appropriate authentication,[41]" which takes multiple use cases into account and evaluates the minimum level of accountability compared to the level of risk involved. Technology decisions should not solely be guided by the authentication terminology like "single-" and "two-factor". In some cases, the former may actually provide higher levels of assurance and accountability than a weaker two-factor method and certainly higher than legacy passwords. Thus, it pays to be cautious in using only risk based, authentication criteria. This ideology strongly advocates for balancing the total justifiable cost with lowest acceptable ease of use.[42] The following should be considered when evaluating authentication methods:

ACCESS POINTS – Merchants need to take all access points into consideration when it comes to authenticating access to sensitive information. Merchants should take special care to securely authenticate mobile, tablets or other devices that can access the network remotely.[43]

IT RESOURCES – multi-layered authentication alone is no easy feat and securing authentication for devices often poses an additional burden. Merchants need to consider integrations, re-integrations and the total cost of securing authentication environments in a way that offers convenience for consumers as well as administrators.[44]

ADMINISTRATION – Authentication should be managed by an administrator with broad, cross channel access to make needed adjustments efficiently. This access includes the need for visibility of customers across all channels as well as automation and central management. The ability to fine-tune authentication requires access to granular reporting and deep insights on which changes can be based.[45]

CUSTOMER EXPERIENCE – Merchants can't afford to forget about this important component to any authentication strategy. While ensuring security protocols are active and enforced, merchants need to look for ways to streamline user access and minimize friction in the checkout process on mobile and other devices. By offering several authentication methods (text to phone, hardware tokens or phone tokens), merchants can offer a convenient way for customers to validate their identity while remaining compliant with internal security protocol.

Look to Your Gateway Partner to Centralize and Streamline Fraud and Risk Prevention in One Flexible and Secure Payment Platform.

Implementing best practices and adhering to industry standards for device authentication takes time and resources. Creating and executing a successful, risk-appropriate authentication strategy requires fine-tuning that many merchants simply don't have the resources to perfect on their own. Working with a third-party vendor can alleviate the resource burden, freeing up merchants to get back to running their business.

SAFE, SECURE PROCESSING ENVIRONMENT WITH COMPREHENSIVE FRAUD PROTECTION BOOSTS CONSUMER CONFIDENCE…AND PROFITS.

Verifi's Global, "Super Gateway" is a secure payment processing platform with robust transaction capabilities and analytics to support merchants of all sizes. Verifi's experience processing more than $20 billion in transactions annually and serving more than 7,000 accounts internationally gives us insight into the unique payment processing needs different companies in different markets face. With support for OVER 70 major domestic and international acquirer and processing networks, our comprehensive platform gives you the freedom and ability to process your payments in the best manner for your business, while minimizing your costs. When it comes to device – or any other – authentication, Verifi's "Super Gateway" facilitates secure payment processing along every step of the transaction lifecycle through a PCI Level 1 certified platform that enables layering and customization of a variety of fraud prevention tools. Verifi's platform supports tokenization and the virtual terminal provides maximum security and control from any computer or location.

COMPREHENSIVE, LAYERED FRAUD PROTECTION ACROSS THE ENTIRE TRANSACTION LIFECYCLE.

Verifi's end-to-end payments protection suite tightly couples our Global "Super Gateway," Intelligence® Suite and chargeback prevention and recovery services so you can protect your revenue streams and process payments more securely and seamlessly. Gateway's Intelligence® Suite provides a comprehensive fraud management platform that enables you to cost-effectively layer, test and adapt best-of-breed tools as the marketplace – and fraudsters – evolve. Our embedded rules engine gives you the ability to centralize and easily accept or decline transactions with pre-set or custom business rules. Merchants can layer and modify multiple fraud prevention tools (device intelligence, geolocation and digital fingerprinting) seamlessly through one integration, to minimize risks without adding IT costs or turning away legitimate sales.

The "Super Gateway" enables Verifi's Total Chargeback Management system, including the award winning Cardholder Dispute Resolution Network™ (CDRN) to stop up to 40% of chargebacks upfront and its Premier Chargeback Representment and Revenue Recovery services to reclaim nearly two times the industry average win rate for profits that would otherwise have been lost to unwarranted chargebacks. Combined, these solutions help stop chargebacks without stopping legitimate sales and provide white glove support for fighting chargebacks that can't be avoided, so merchants can focus their time, resources and effort on what matters – building their business and boosting profits.

The "Super Gateway" also enables Verifi's Decline Salvage billing services to recapture customers and billings you might otherwise have lost to preventable card declines. Merchants using Decline Salvage improve authorization rates and retain loyal customers by up to 20% - customers that produce an average of 150% more in revenue just one year later.

Conclusion

There's no simple solution when it comes to authentication for devices. According to Statista, there will be more than 1.7 billion consumers with smartphones by 2018, making multi-layered device authentication absolutely necessary.[46] Each business has unique needs and a unique business model to which fraud and security controls must be tailored while also taking into account consumer convenience. Mobile remote and proximity payments will continue to grow, prompting additional security measures to garner consumer trust and adoption and to protect payments across all channels. Omni-channel merchants must balance a secure purchasing experience with a positive purchasing experience, taking into account the trade-offs between security and convenience and considering the total cost of each. The considerations outlined in this white paper should help merchants evaluate their current processing gateway and validate if it is agile enough to adapt to changing opportunities and security demands as fraudsters become more educated, dynamic and voracious in the CNP channel.

About Verifi

Verifi, an award-winning provider of end-to-end payment protection and management solutions, was founded in 2005 to help our clients effectively manage the payments challenges they face everyday. Verifi helps merchants safely process payments, combat fraud, prevent and resolve costly chargebacks, as well as increase billings and keep loyal customers. Our best-in-breed solutions and white glove support are trusted by a wide range of industries from emerging companies to the Fortune 500. Headquartered in Los Angeles, California, we process more than $20 billion transactions annually and currently serve more than 7,000 accounts internationally.

VERIFI™

For More Information

Main Phone: (323) 655-5789 Mon-Fri 8:00 AM – 5:00 PM PST
Main Fax: (323) 655-5537
Email Address: info@verifi.com
Mailing Address: 8391 Beverly Blvd., Box #310, Los Angeles, CA 90048

Citations

1 https://www.pingidentity.com/en/blog/2014/04/24/securing_identity_in_the_omnichannel_an_infographic.html

2 http://www8.hp.com/us/en/hp-news/press-release.html?id=1815969#.VVDQn_lViko

3 http://www.chainstoreage.com/article/six-steps-boost-data-security-protection

4 http://aitegroup.com/report/e-commerce-and-cnp-transactions-explosive-growth-explosive-risk

5 http://aitegroup.com/report/e-commerce-and-cnp-transactions-explosive-growth-explosive-risk

6 https://www.internetretailer.com/2015/02/17/us-annual-e-retail-sales-surpass-300-billion-first-ti

7 http://www.acfe.com/rttn-small-businesses.aspx

8 http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf

9 http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf

10 https://www.forrester.com/US+Mobile+Payments+To+Reach+142+Billion+By+2019/-/E-PRE7454

11 http://www.csoonline.com/article/2880119/mobile-security/survey-average-company-losing-90-million-to-mobile-fraud.html

12 http://www.pymnts.com/news/2015/ingenico-and-intel-tie-up-for-payments-on-the-internet-of-things/#.VUtjp0tkf8E

13 http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en

14 http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en

15 http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en

16 http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en

17 http://www.informationsecuritybuzz.com/three-five-use-password-across-multiple-online-accounts/

18 http://www.aitegroup.com/report/3-d-secure-poised-live-long-and-prosper

19 http://www.aitegroup.com/report/3-d-secure-poised-live-long-and-prosper

20 http://www.aitegroup.com/report/3-d-secure-poised-live-long-and-prosper

21 http://www.cbronline.com/blogs/cbr-rolling-blog/deploy-strong-authentication-using-a-multi-layered-security-strategy

22 http://www.cbronline.com/blogs/cbr-rolling-blog/deploy-strong-authentication-using-a-multi-layered-security-strategy

23 http://www.cbronline.com/blogs/cbr-rolling-blog/deploy-strong-authentication-using-a-multi-layered-security-strategy

24 http://www.smashingmagazine.com/2011/03/04/in-search-of-the-perfect-captcha/

25 http://searchsecurity.techtarget.com/feature/The-fundamentals-of-MFA-Multifactor-authentication-in-the-enterprise

26 http://usa.visa.com/download/merchants/global-visa-card-not-present-merchant-guide-to-greater-fraud-control.pdf

27 http://usa.visa.com/download/merchants/global-visa-card-not-present-merchant-guide-to-greater-fraud-control.pdf

28 http://arstechnica.com/security/2013/10/top-sites-and-maybe-the-nsa-track-users-with-device-fingerprinting/

29 http://www.informationweek.com/mobile/zeus-banking-trojan-hits-android-phones/d/d-id/1098909?

30 http://www.fico.com/en/blogs/fraud-security/cyber-talk-can-fraud-protection-analytics-stop-cyber-crime/

31 https://check.torproject.org/cgi-bin/TorBulkExitList.py

32 http://insights.mobify.com/top-6-reasons-your-shopping-cart-abandonment-rate-is-high-on-mobile-and-how-to-fix-it/ and http://www.forbes.com/sites/neilpatel/2014/09/23/improve-your-online-checkout-process/

33 http://baymard.com/lists/cart-abandonment-rate

34 http://blog.riskified.com/true-cost-declined-orders/

35 http://blog.riskified.com/true-cost-declined-orders/

36 *http://gimmeanother.com/retailers/mobile-shopping-cart-abandonment-rates-giving-nightmares/*

37 *http://www.computerweekly.com/opinion/Gartner-What-matters-is-risk-appropriate-authentication*

38 *http://www.computerweekly.com/opinion/Gartner-What-matters-is-risk-appropriate-authentication*

39 *http://www.computerweekly.com/opinion/Gartner-What-matters-is-risk-appropriate-authentication*

40 *https://www.chase.com/content/dam/chasecom/en/commercial-bank/executive-connect/common/document/afp-payments-fraud-results.pdf*

41 *http://www.computerweekly.com/opinion/Gartner-What-matters-is-risk-appropriate-authentication*

42 *http://www.computerweekly.com/opinion/Gartner-What-matters-is-risk-appropriate-authentication*

43 *http://www.safenet-inc.com/multi-factor-authentication/strong-authentication-best-practices/*

44 *http://www.safenet-inc.com/multi-factor-authentication/strong-authentication-best-practices/*

45 *http://www.safenet-inc.com/multi-factor-authentication/strong-authentication-best-practices/*

46 *http://www.statista.com/statistics/263441/global-smartphone-shipments-forecast/*