WHITE PAPER

Smart Card Alliance

Payments Council

A SMART CARD ALLIANCE PAYMENTS COUNCIL WHITE PAPER

The True Cost of Data Breaches in the Payments Industry

Publication Date: March 2015
Publication Number: PC-15001

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

Copyright © 2015 Smart Card Alliance, Inc. All rights reserved. Reproduction or distribution of this publication in any form is forbidden without prior permission from the Smart Card Alliance. The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report. This white paper does not endorse any specific product or service. Product or service references are provided to illustrate the points being made.

Table of Contents

1 Introduction

As has been reported widely, data breaches are a growing problem globally, with every industry sector affected by breaches. This white paper was developed by the Smart Card Alliance Payments Council to focus on the costs that are relevant to payments industry stakeholders – issuers, merchants, acquirers and processors – and their cardholder customers. The white paper provides a resource that can be used by stakeholders to identify and estimate the total cost of a data breach.

"Nearly a billion records were compromised in 2014." *NetworkWorld, November 17, 2014*

"Target Says Credit Card Data Breach Cost It $162M In 2013-14," *TechCrunch, February 25, 2015*

"The financial consequences of Anthem's massive data breach could reach beyond the $100 million mark," *CNET, February 12, 2015*

The white paper includes the following topics:

- Definition of data breach
- Recent data breach statistics and reported costs
- Definition of both quantifiable and intangible costs that need to be considered when calculating the total cost of a data breach
- Identification of the stakeholder impact for different costs

Through an analysis of potential costs and use of the tools referenced in this white paper, payments industry stakeholders can understand the true impact a data breach might have on their organization. In addition, this can help organizations create the business case for developing a proactive data breach prevention strategy and for creating breach reaction tools.

2 What Is a Data Breach?

ISO/IEC Standard 27040 defines a data breach as a "compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data that is transmitted, stored, or otherwise processed." In other words, a data breach results in the intentional or unintentional loss of secure or personal information. Data breaches can involve any kind of data: financial information, individual identity information—even data that is considered to be intellectual property.

Data breaches typically result when an individual or group of individuals accesses a logical or physical infrastructure, including hard drives or database information that may be stored unencrypted. Bank card data breaches are usually achieved through one or more of the following:

- A skimming device
- Malware that infiltrates the computer system that manages or processes banking or personal information
- A phishing website
- Key logging to steal PIN data
- A listening device that taps into telephone lines to intercept unencrypted information
- Employee negligence
- System failure

Most bank card data breaches are a result of skimming or a database compromise which can occur due to one of the methods listed above. Traditionally, skimming requires the installation of a physical device, most commonly at an unattended location, such as an ATM. A total of 87 percent of reported skimming attacks occurred at unattended ATMs.[1] Data can also be skimmed logically, using wireless Bluetooth devices or by replicating the database records that temporarily hold payment card data. Other recent major data breaches resulted from malware installed in backend computer systems or databases that access and copy valuable data to other systems. Regardless of the source, the data is sold to interested parties and used illegally.

Recent statistics on data breaches are startling:

- In the first 9 months of 2014, 904 million records were compromised in 1,922 confirmed incidents. Many of the incidents reported in 2014 involved record-setting amounts of data, including 20 incidents that compromised more than 1 million records each.[2]

- The number of U.S. data breaches tracked in 2014 hit a record high of 783 in 2014, according to a recent report by the Identity Theft Resource Center (ITRC) and sponsored by IDT911™. This represents a substantial hike of 27.5 percent over the number of breaches reported in 2013 and a significant increase of 18.3 percent over the previous high of 662 breaches tracked in 2010. The number of U.S. data breach incidents tracked since 2005 also hit a milestone of 5,029 reported data breach incidents, involving more than 675 million estimated records. This equated to 15 breaches each week in 2014. This press release even foretold 2015 with the statement, "Without a doubt,

[1] Verizon, *2014 Data Breach Investigations Report*. http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf.

[2] Steve Ragan, "Nearly a billion records were compromised in 2014," *Network World*. http://www.networkworld.com/article/2848479/security0/nearly-a-billion-records-were-compromised-in-2014.html.

2015 will see more massive takedowns, hacks and exposure of sensitive personal information like we have witnessed in years past."[3]

- 2015 data through March 11, 2015 indicate 150 breaches and over 88 million records compromised.[4]

[3] http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html

[4] http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReportSummary2015.pdf

3 Costs Associated with Data Breaches

The costs of data breaches have also increased. The 2014 Ponemon Study cited that "the average cost for each lost or stolen record containing sensitive and confidential information increased from $188 to $201. The total average cost to involved organizations increased from $5.4 million to $5.9 million."[5] Their study, in its eleventh year, shows data from breaches occurring mostly in 2013. Cost per compromised record related to data breaches put financial services data breaches in the top five; health care, with a cost per compromised card of $316, is number one.

Rising costs, coupled with steadily increasing incident reports, make awareness of the types of attacks and tools used to defend against such attacks imperative. Various statistics have been published on the cost of breaches.

- One statistic indicates that in Ohio, credit unions spent over $1.3 million in the wake of the Home Depot data breach. The costs were mostly related to reissuance of cards and responding to fraudulent charges.[6] The same study reported that Alabama credit unions also posted over $1 million in costs because of the Home Depot breach.
- The per-card-issued cost was $8.02, which includes the costs of new cards, fraud, additional staffing, member notification, account monitoring, and more.[7]
- All told, the Home Depot and Target data breaches combined have cost credit unions and members nearly $100 million dollars in the last year.[8]

The cost to merchants is also high. According to *USA Today*, "The company [Target] is still recovering financially. The breach has cost the company $148 million, minus a $38 million insurance payment. Profits for the first six months of their fiscal year were down 41% from the same period a year ago."[9]

The variance in the above examples illustrates the need for a standardized approach to calculating the true cost of data breaches.

This topic – exactly what costs should a company consider when calculating the total cost of a breach – is what brought this white paper to light. Costs will apply to some stakeholders and not to others. Also, some costs may be extremely difficult to quantify, like the cost of brand damage. Some of the costs associated with data breaches are well defined; others are somewhat challenging to capture fully.

Examples of costs that will be difficult to fully capture include:

- Recoupment of disputed transactions
- Intangible cost associated with card replacement
- Loss of existing customers or a decline in new customer acquisitions

---

[5] Ponemon Institute LLC, *2014 Cost of Data Breach Study: United States*, May 2014, http://essextec.com/sites/default/files/2014%20Cost%20of%20Data%20Breach%20Study.PDF.

[6] "Ohio credit unions spend $1.3 million on Home Depot data breach," *The Columbus Dispatch*, Nov. 3, 2014, http://www.dispatch.com/content/stories/business/2014/11/03/ohio-credit-unions-spend-1-3-million-on-data-breach.html.

[7] Lucy Berry, "What did Home Depot data breach cost Alabama credit unions? Nearly $1M, survey says," Nov. 3, 2014, http://www.al.com/business/index.ssf/2014/11/what_did_massive_home_depot_da.html.

[8] Michael Bridges, "Home Depot breach costs double the Target costs," LCSU (League of Southeastern Credit Unions) & Affiliates, http://www.lscu.coop/Communication-Press-Room/News-Feed/Top-Stories/Home-Depot-breach-costs-double-the-Target-costs.

[9] Hadley Malcolm, "Target leaves breach behind this holiday season," *USA Today*, Oct. 21, 2014, http://www.usatoday.com/story/money/business/2014/10/21/target-holiday-plans/17663057/.

- Increased labor due to customer inquiries
- Legal fees
- Credit counseling for affected customers
- Promotional campaigns aimed at recovering customers and rebuilding trust/loyalty
- Contractual obligations to customers, partners, and others that include performance penalties that also result in audits

Costs can be increased if the breach involves any of the following:

- Engaging consultants to support the incident response team
- Replacing lost or stolen physical assets (devices)
- Notifying customers
- Handling third-party errors

Certain factors can decrease the costs associated with a data breach:

- A strong security posture (i.e., a proactive approach to preventing breaches)
- An in-place, reviewed incident response plan
- Chief information security officer (CISO) leadership

3.1 Cost Definition and Details

The first step in determining the true cost of a breach is to fully understand the breadth of costs to consider and use a standard definition of what should be included. Table 1 lists and defines the potential costs of a data breach.[10]

Table 1. Costs Applicable to Data Breaches

Cost	Description
Audits	An audit is a systematic and independent examination of data, statements, records, operations, and performances (financial or otherwise) of an enterprise for a stated purpose. Costs may be incurred for any post-breach audits required by customers or other organizations, including the costs of the annual PCI audits by stakeholders.
Brand	While a brand is defined as an intangible asset, it is often the most valuable asset on a corporation's balance sheet. Brand owners manage their brands carefully to create shareholder value, and brand valuation is an important management technique that ascribes a money value to a brand. Breaches can damage the company brand and reputation.
Call center	A call center is centralized office used for the purpose of receiving or transmitting a large volume of requests by telephone. Costs can include rescripting call screens for employees, managing more or longer calls, and providing additional education and training for employees.

[10] Definitions from Wikipedia, updated with industry specific content or examples.

Cost	Description
Card reissuance	Direct costs include getting a replacement card to the cardholder: purchasing the card plastic, personalizing the card, and delivering the card to the cardholder (e.g., insert and postage costs). Ancillary costs include the management of the reissuance process with vendors, rush fees for faster production, overnight delivery fees for some cardholders, and other charges.
Chargebacks	A chargeback is initiated when a cardholder formally disputes a transaction, stating that they do not recognize the transaction or that the merchant did not live up to their obligation. The chargeback process is guided by payment network regulations. Typically a merchant would be required to supply proof, such as a signature, that the customer did indeed make the transaction. If the dispute is resolved in favor of the merchant, the cardholder is obligated to pay the charge. Otherwise the transaction is charged back to the merchant. Time is required for issuer employees to work with merchants and cardholders to review and process chargeback transactions. The chargeback process involves costs to the issuer, acquirers and merchants. Chargebacks may be a source of irritation and brand damage to customers.
Communications	Communication costs are spread throughout a variety of areas. Each stakeholder must take time to understand the required communications and their costs. For example, for issuers this cost can include sending notices and updating call center and front line staff and websites. For merchants, this cost can include media and e-mail communications to customers. Stakeholders should assess who must be communicated with and what costs will be incurred.
Criminal pursuit and prosecution	The cause of the breach must be investigated to determine who was responsible. Once a perpetrator is found, there are also costs of prosecution. These costs may be shared between merchants, financial Institutions, payment brands, and other parties.
Credibility	Credibility involves the objective and subjective components that contribute to the believability of a source or message. Credibility has two key components: trustworthiness and expertise. Data breaches can create consumer unease with merchants and issuers. Damage to credibility should be calculated in the cost of brand damage.
Credit monitoring	Credit monitoring can help detect credit-related fraud and identity theft, typically providing regular access to an individual's credit history, alerts of critical changes to the credit history, and additional services. After a data breach, companies may offer credit monitoring services on a subscription basis to affected cardholders; the breached party will typically pay to provide this service to affected cardholders for a period of at least one year.
Credit rating	A breach may impact an organization's credit rating, affecting their ability to raise new funds, and may inhibit new investment opportunities.

Cost	Description
Customer pain	This is a catchall category for any issues the consumer is experiencing because of the data breach: for example, having no card to use for purchases; ordering something with a card that was in a system that is now cancelled; moving recurring payment transactions to a different card; working with issuers on chargebacks; and dealing with other pain inflicted by this inconvenience.
Customer service	This is a catchall category for the costs incurred by customer-facing staff across an organization to handle consumers after a breach has occurred. This includes the "good will" activity that needs to occur to appease the customer and retain the customer relationship and loyalty, which can affect brand equity as well. Call center costs can be included or calculated separately. This cost can include extra staffing to work with consumers.
Declined transactions	Declined transactions can result from tightened fraud scoring rules in the wake of a breach or from a card being shut down by the issuer due to a data breach. Each transaction processed generates a fee to the merchant from the acquirer and/or payment brands. When a cardholder uses a card and the transaction is declined, the merchant is still charged to process the transaction. The consumer also is inconvenienced in not being able to pay using the preferred method of payment and may lose rewards or loyalty points. Declined transactions can also influence brand equity for any companies that the consumer perceives are involved in the transaction.
Educational outreach	A breached organization may invest or may be required to invest in new educational outreach programs to raise awareness of security threats and/or improve its public image.
Equipment and system updates	POS equipment and/or back-end systems will need to be updated to incorporate new security solutions.
Executive time	This is the cost of the mind share spent by executive leadership thinking about, planning and responding to a breach. This cost can also include time allocated for government reviews, internal discussions, public relations efforts, audits, and vulnerability assessment reviews.
Expedited shipping	Shipping costs can increase, depending on how an issuer sends cards to consumers and whether shipping must be expedited. Additional costs can range from $10 to $30 per person for domestic deliveries and up to $200 for International deliveries.
Fees/fines	Under some contractual relationships, a party or a party's service provider agrees to pay a noncompliance fee if noncompliance is discovered as part of a data breach investigation.
Forensic audit	Forensic audits examine and evaluate a firm's or individual's financial information for use as evidence in court. A forensic audit can be conducted in order to prosecute a party for fraud, embezzlement, or other financial crimes.

Cost	Description
Fraud analysis	This cost is incurred if cardholders have to review transactions with the issuer to determine which transactions are fraudulent. This is the cost of case management for high risk transactions.
Fraud response planning	These are the costs incurred by the issuer to determine a reissuance strategy and tag affected cards, manage communication, and reach affected customers.
Fraud scoring	Fraud scoring calculates the riskiness of authorizing a payment, or, for e-commerce merchants, accepting an order. Banks and merchants use transaction data and history along with rules and analytical tools to predict the likelihood that a transaction is fraudulent, and then determine whether to approve, decline or review the transaction. Fraud scoring generally identifies transactions that appear to be uncharacteristic of a customer's behavior, occur in a risky geography, encompass fraud-prone merchandise or merchants, have suspicious IP or email addresses, have mismatched billing and delivery physical addresses, or follow some new suspicious pattern. As a result of the fraud score, merchants may attempt to verify addresses or card verification value. After a data breach, merchants and issuers may need to update the scoring process.
Generation of card reissuance files	This is the cost to the issuer to generate card reissuance files and generate new primary account numbers (PANs). The PANs are used to create an embossing file that is sent to the card personalization center for production. After this process, issuers would also have the card reissuance cost defined above.
Goodwill	This is described as the value of a business entity not directly attributable to its assets or liabilities. In the case of a data breach, a company could have an increase in negative media attention that could impact the value of the company's goodwill.
Human resources	Human resources must address staffing issues raised by responding to a breach, including re-hiring staff or temporarily staffing certain customer-facing areas.
Insurance fees	After a breach, insurance claims can be filed by the policy holder (e.g., merchant breached), which can result in increased fees when the policy is renewed. Insurers may also raise fees across a segment of policy holders.
Issuer fees	Issuers may charge cardholder fees as a result of fraudulent activity. For example, if the fraud involves a debit card, cardholders may incur insufficient fund fees or overdraft protection fees. These fees would have to be refunded to the cardholder, resulting in manual effort and rework on the part of the issuer. If not handled correctly this can be a significant source of anxieity and irritation for cardholders, resulting in further brand damage.
IT costs	If the IT system is found to represent a risk during breach investigation, there can be costs to review and fix the issues. These costs can include the costs of any auditing or monitoring that should have been done prior to the breach.

Cost	Description
Law enforcement	These are the costs to government agencies that investigate the breach and prosecute the fraudsters.
Legal fees	History shows that after a breach, multiple lawsuits may be filed. The cost of filing lawsuits and defending against lawsuits should be considered in any cost calculation of a data breach; they can be quite substantial.
Liability for cost of fraudulent transactions	Currently, issuers are mainly responsible for the costs of the card-present fraudulent transactions, while merchants are generally responsible for card-not-present transactions. After the EMV fraud liability shift date, these costs could be transferred to the weakest link in the payment chain, based on payment brand guidelines.
Loss of spend	There is a time period after a breach but before an affected cardholder receives a new card during which loss of consumer spend can occur. For merchants, a cardholder may not know that the card has been turned off or may not have another payment vehicle to use to make a purchase. Another consideration for a merchants involved in data breaches is the potential decline in transaction volume resulting from bad publicity. For issuers, there is an interchange fee loss if the consumer uses another payment vehicle to make a purchase.
Loss of "top of wallet" status	Issuers focus on making their card product the payment vehicle of choice for consumers. Any impact on the usability of the card can damage the top of wallet status.
Lost revenue	Any stakeholder in the payment ecosystem can lose revenue due to consumer and issuer response to a breach.
Market valuation	A breach may have impact on the market valuation (i.e., stock price) of the breached organization and require increased focus on investor relations.
Merchant staff time	Merchants will need to dedicate staff to handle calls and customer requests, respond to investigators' questions, and inform employees after a breach occurs that could originate in their system.
New staff	Stakeholders in the payment ecosystem may need to add fraud- and risk-management staff and may have management changes and reorganization.
Opportunity cost	Handling a breach requires attention from the entire organization, which distracts from day-to-day operations, pre-breach priorities and other business opportunities.
Penalties	See fees/fines.

Cost	Description
Penetration test	A penetration test simulates an attack with a specific goal, like accessing personal account data behind a firewall. A typical goal could be to access the contents of the customer database on the internal network. The deliverable for a penetration test is a report of how security was breached in order to reach the agreed-upon goal (and often how to remediate).
PR and marketing efforts	When a breach announcement identifies a potentially liable party, that party will need PR and marketing efforts to retain customer support and minimize reduction in sales volumes.
Recurring payment changes	Cardholders who have set up recurring transactions on a payment card will need to contact the merchant that receives the payment and update the payment card data. There is time involved for the cardholder and potentially an annoyance factor if a cardholder forgets to update a payment. Additional time and expense can be required to address issues that result from missed payments, such as late fees or service cancellations. Merchants with large numbers of recurring payments may incur costs to identify and contact customers who have not updated their data. Issuers may see long term revenue reduction if consumers move their recurring payments to a different issuer's product.
Relationships with regulators and business partners	A breached organization will have to invest effort to satisfy regulators and business partners and demonstrate progress to retain security certifications.
Scrubbing customer files	Issuers incur costs to identify affected customers, scrub data records to determine the extent of fraudulent activity, and eliminate unaffected customers to create a list of customers to whom new cards must be reissued. This is related to the cost of generating card reissuance files.
Settlement fees	These are the payments required after settlement of lawsuits.
System outages	During breach recovery, system outages may be necessary to resolve identified issues. Costs associated with upgrades should be included in IT costs, but down time also needs to be accounted for.
Training	Stakeholders who are liable for a breach will typically implement new policies governing security or compliance or both. Employee training will be required. Parties affected by the breach also incur training costs when new processes or procedures are implemented in response to the data breach.
Security upgrades	Security upgrade costs can include the indirect cost of upgrading security policies, defenses, or technologies in reaction to a breach or a regulatory threat.
Vulnerability assessment	A vulnerability assessment identifies, quantifies, and prioritizes (or ranks) the vulnerabilities in a system. Such an assessment is designed to yield a prioritized list of vulnerabilities.

3.2 Impact Matrix

The second step in the process is to determine which stakeholder group the company falls into or whether a cost model should be created. This white paper breaks costs into those experienced by acquirers, merchants, issuers, cardholders, payment brands and others. The matrix took into account the following for each stakeholder.

- Acquirer. Each time someone uses a debit or credit card, the service of an acquirer is used. The acquirer processes credit or debit transactions on behalf of a merchant and then settles approved transactions, by placing funds into the sellers' account.
- Merchant. This is the seller in a transaction. The merchant can be a brick-and-mortar business or an Internet business. A merchant is basically anyone who trades goods or services in exchange for payment.
- Issuer. The issuer is the company that provides a credit, debit or prepaid payment card to a cardholder.
- Cardholder. This is the user of the payment medium who could be impacted by a data breach.
- Payment brand. This is the payment network whose brand appears on the payment card.
- Other. This category includes other stakeholders that could be impacted but are not considered the main focus on this white paper. This can include law enforcement, government agencies and insurance companies, to name a few.

After the stakeholder group is determined, the impact matrix in Table 2 below can be used to determine the costs that should be considered when calculating the true cost of a breach. Please note that just because the matrix doesn't indicate a cost relates to a specific stakeholder group, it may apply and should be included in the calculation.

Table 2. Impact of Data Breach Costs on Stakeholders

Cost	Acquirer	Merchant	Issuer	Card-holder	Payment Brand	Other
Audits	✓	✓	✓		✓	✓
Brand	✓	✓	✓		✓	
Call center	✓	✓	✓			✓
Card reissuance		✓	✓	✓		
Chargebacks	✓	✓	✓	✓		✓
Communications	✓	✓	✓		✓	
Criminal pursuit and prosecution	✓	✓	✓	✓	✓	✓
Credibility	✓	✓	✓		✓	✓

Cost	Acquirer	Merchant	Issuer	Card-holder	Payment Brand	Other
Credit monitoring	✓	✓	✓			
Credit rating	✓	✓	✓		✓	
Customer pain				✓		
Customer service	✓	✓	✓			
Declined transactions	✓	✓				
Educational outreach	✓	✓	✓		✓	
Equipment and system updates	✓	✓	✓			
Executive time	✓	✓	✓		✓	
Expedited shipping		✓	✓			
Fees/fines	✓	✓	✓	✓	✓	
Forensic audit	✓	✓	✓		✓	
Fraud analysis			✓	✓		
Fraud response planning			✓			
Fraud scoring		✓	✓			
Generation of card reissuance files			✓			
Goodwill		✓	✓		✓	
Human resources	✓	✓	✓		✓	✓
Insurance fees	✓	✓	✓		✓	✓
Issuer fees			✓	✓		

Cost	Acquirer	Merchant	Issuer	Card-holder	Payment Brand	Other
IT costs	✓	✓	✓		✓	✓
Law enforcement	✓	✓	✓		✓	✓
Legal fees	✓	✓	✓		✓	
Liability for cost of fraudulent transactions		✓	✓			
Loss of spend		✓	✓			
Loss of “top of wallet” status			✓			
Lost revenue	✓	✓	✓		✓	✓
Market valuation	✓	✓	✓		✓	
Merchant staff time		✓				
New staff	✓	✓	✓		✓	✓
Opportunity cost	✓	✓	✓		✓	✓
Penalties	✓	✓	✓		✓	✓
Penetration test	✓	✓	✓		✓	
PR and marketing efforts		✓	✓		✓	✓
Recurring payment changes		✓		✓		
Relationships with regulators and business partners	✓	✓	✓		✓	✓
Scrubbing customer files		✓	✓			
Settlement fees	✓	✓	✓			✓

Cost	Acquirer	Merchant	Issuer	Card-holder	Payment Brand	Other
System outages	✓	✓	✓		✓	
Training	✓	✓	✓		✓	✓
Security upgrades	✓	✓	✓			✓
Vulnerability assessment	✓	✓	✓		✓	

4 Conclusions

The goal of this white paper was to establish a clear definition of what constitutes a data breach and to identify the cost categories that are impacted when a breach occurs. Issuers, acquirers, merchants, cardholders and payment brands have all been impacted to a degree by breaches. The impact and costs associated with each breach are unique. Additional outside resources are available to calculate the actual financial impact referenced below

To understand the financial impact of a data breach the ecosystem must be understood, so that all of the components are considered. The terms and outline of data breach costs in this white paper were developed to help with the itemization of the costs associated with a breach and assist in determining a final economic impact.

As demonstrated by the extensive costs discussed in this white paper, upfront prevention of data breaches is always the best approach. Investing upfront in security and breach prevention and response technologies can help to prevent or detect breaches and reduce the cost if a breach occurs.

Additional references can be found at:

http://www.databreachcalculator.com/GetStarted.aspx

http://www.idt911.com/expensecalc/start.aspx/

http://www.privacyrisksadvisors.com/data-breach-toolkit/data-breach-calculators/

http://www.ibmcostofdatabreach.com/

5 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Payments Council to provide an educational resource on the potential costs that could be incurred during a data breach. The white paper consolidates industry information on categories of costs as a reference document.

Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Payments Council members for their contributions. Participants involved in the development of this white paper included: ABnote; American Express; Capgemini; CH2M HILL; Chase; CPI Card Group; First Data Corporation; Fiserv; Giesecke & Devrient; Heartland Payment Systems; Infineon Technologies; Ingenico; Initiative for Open Authentication (OATH); INSIDE Secure; Intelcav; JCB International Credit Card Co., Ltd; NXP Semiconductors; Oberthur Technologies; OTI America; Tyfone; Verifone; Visa Inc.; Wells Fargo

The Smart Card Alliance thanks **Docia Myer**, CPI Card Group, for leading the project, and the following Council members who wrote content and participated in the project team for this document:

- **Philip Andreae**, Oberthur Technologies
- **Louis Bianchin**, Intelcav
- **Jose Correa**, NXP Semiconductors
- **Brady Cullimore**, American Express
- **Michael English**, Heartland Payment Systems
- **Allen Friedman**, Ingenico
- **Reid Holmes**, INSIDE Secure
- **Tony McGee**, CPI Card Group
- **Cathy Medich**, Smart Card Alliance
- **Docia Myer**, CPI Card Group
- **Sharon Pazlar**, Fiserv
- **Nick Pisarev**, Giesecke & Devrient
- **John Smith**, First Data
- **Brian Stein**, CH2M HILL
- **Sree Swaminathan**, First Data

The Smart Card Alliance also thanks Payments Council members who participated in the review of the white paper including:

- **Steve Arebalo**, INSIDE Secure
- **Deborah Baxley**, Capgemini
- **Scott Hagstrom**, ABnote
- **Peg Heuer**, Wells Fargo
- **Nizar Jamal**, Tyfone
- **Julie Krueger**, JCB
- **Don Malloy**, OATH
- **Arnaud Moser**, Infineon Technologies
- **Bill Norwood**, Heartland Payment Systems
- **Lokesh Rachuri**, Capgemini
- **JC Raynon**, Verifone
- **John Rego**, OTI America
- **Joe Scott**, Visa Inc.
- **Paul Simon**, Chase
- **Jamie Topolski**, Fiserv

Trademark Notice

All registered trademarks, trademarks, or service marks are the property of their respective owners.

About the Smart Card Alliance Payments Council

The Smart Card Alliance Payments Council focuses on facilitating the adoption of chip-enabled payments and payment applications in the U.S. through education programs for consumers, merchants, issuers, acquirers/processors, government regulators, mobile telecommunications providers and payments service providers. The group is bringing together payments industry stakeholders, including payments industry leaders, merchants and suppliers, and is working on projects related to implementing EMV, contactless payments, NFC-enabled payments and applications, mobile payments, and chip-enabled e-commerce. The Council's primary goal is to inform and educate the market about the value of chip-enabled payments in improving the security of the payments infrastructure and in enhancing the value of payments and payment-related applications for industry stakeholders. Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects.