Data Security

Made Simpler

Sponsored by VISA symantec. KROLL

Published January 2010

Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Data Security - *Made Simpler*

Sponsored by VISA symantec. KROLL

IT'S ABOUT TRUST

Nothing is more important to you as a small business owner than your customers. You've worked hard to engage and secure their trust and confidence in you, and growing your business will depend in large part on maintaining their trust. In today's competitive marketplace, that's more difficult to do than ever.

As hard as you've worked to earn your customers' trust, it can take just one negative experience to break it. ***Your ability to keep your customers' sensitive data secure is one of those make-it-or-break-it events.*** It may surprise you, but developing a data protection plan — and then openly communicating it and actively implementing it — is a key way to *build* customer trust. Today's savvy buyers actively look for tangible signs that a business they're interacting with has taken the necessary precautions to secure their sensitive customer data. If they're not confident that you'll protect their data, they won't do business with you. Many online buyers will abandon the transaction process if they don't have confidence in the online retailer.

Protecting Your Data vs Becoming a Statistic

We've all seen the headlines in recent years about large scale data breaches — an international crime ring hacks into a national retailer, siphoning off millions of payment card details; or a government agency loses millions of personal records that include Social Security Numbers. These types of data losses can happen to small businesses as well, although they don't always lead to national headlines. ***In fact, Visa estimates that approximately 85% of data breaches occur at the small business level.***

Taking proactive, strategic steps to protect your customer and employee data — and developing a plan for how you would respond should something occur that compromises that data — will:

- Strengthen the trust that your customers place in you
- Set you apart from your competition
- Save you money in the near-term
- Might even save your business in the event of a significant data loss

BBB's Data Security – *Made Simpler* is here to help address these issues. Data security is not a simple issue to address...but in this Guide, we've tried to make the information:

- *Simpler* to read,
- *Simpler* to process, and
- *Simpler* to help you get your data security house in order.

It's written specifically for small business owners, focusing on the most common data security issues small business owners face. It goes beyond telling you what you should be doing; it gives you *concrete guidelines, and turn-key suggestions* that will point you towards s*olutions and resources that are right-sized for small business owners.*

Now let's get started.

KELLEY DRYE BRYAN CAVE Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Data Security - *Made Simpler*

Sponsored by VISA symantec. KROLL

Table of Contents

Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Data Security - *Made Simpler*

Sponsored by VISA symantec. KROLL

1. SECURING SENSITIVE DATA. Start With The Basics.

Customers expect that ***every business*** – large or small – that collects their sensitive personal information will protect it. Beyond customer expectations, there's the law. Depending on your type of business and the states in which your customers reside, you may be legally required to protect the personal information you collect.

30% of security violations come from inside the organization.

Source: 2009 Open Security Foundation report.

Getting Started

First, determine what makes sense for your type of business. This will be based on the type of data that you collect and store, and the kind of resources you have managing that data.

If your small business keeps information about customers in several formats (e.g., on paper, on computers, and online), you should sit down with a team of your employees — an IT person, office manager, etc. — and discuss these issues together to make sure you consider all viewpoints.

1. Inventory the *types* of data you collect, store and/or transmit.

- ❑ Name
- ❑ Physical address
- ❑ Phone numbers
- ❑ Email addresses
- ❑ Account numbers
- ❑ Invoice numbers
- ❑ Social Security Number
- ❑ Driver's License Number
- ❑ Business ID Number
- ❑ Types and amounts of transactions

2. Inventory HOW you store your data.

- ❑ Paper invoices
- ❑ Paper mailing lists
- ❑ Email lists
- ❑ Paper customer files
- ❑ Paper order requests
- ❑ Email
- ❑ Data bases
- ❑ Spreadsheets
- ❑ Customer accounts
- ❑ Customer Lists
- ❑ Contracts
- ❑ Business Plans
- ❑ Financial Reports

3. Inventory *WHERE* you store your data for each type and format of customer information.

PHYSICAL Storage Sites

- ❑ Desk drawers
- ❑ Filing cabinets
- ❑ Mail room
- ❑ Home offices

ELECTRONIC Storage Sites

Endpoints

- ❑ Desktop computer
- ❑ Laptop
- ❑ Servers

Mobile Devices

- ❑ PDAs
- ❑ Cell Phones
- ❑ mp3s
- ❑ USB/Thumb Drives
- ❑ CDs, DVDs
- ❑ Other flash memory devices

KELLEY DRYE BRYAN CAVE Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

4. Inventory *HOW DATA IS MOVED* and *WHO HAS ACCESS to it.*

Take into consideration your type of business, the stationary and portable tools your employees use to do their jobs. This is a very important part of the inventory process, as it will help you begin to identify the potential ways that sensitive data could be inadvertently disclosed. If you think you need outside help to identify potential leak points, consider consulting with a data forensics team or the bank or processor that provides your merchant account services.

Data Access & Flow Checklist

	Connected or Networked?	Who Has Access?	Does it Leave the Office?	Is it Accessible Off-site?	Does it Provide Internet/Email Access?
Endpoints					
❑ Desktop					
❑ Laptop					
❑ Servers					
Mobile Devices					
❑ PDAs					
❑ Cell Phones					
❑ mp3s					
❑ USBs					
❑ CDs, DVDs					
❑ Other flash memory					

5. Inventory the *DATA CONTROLS YOU HAVE IN PLACE…OR NOT*

Control/Protection Tools Checklist

	No	If Yes…How?
❑ Computer Operating System has all current updates and patches – on all machines?		
❑ All endpoint computers have all security devices activated and up-to-date?		
❑ Data encryption in place – on all machines?		
❑ Electronic data is automatically backed up and can be restored in the event of human error, system failure or natural disaster?		
❑ Sensitive data protected from leaving the business network via outbound email?		
❑ Anti-phishing protections in place?		
❑ You and your employees know how to recognize – and avoid – phishing emails that may enter via business or personal email accounts?		
❑ Malware protections for what may try to enter via:		
o Business email accounts?		
o The Internet (i.e., web browsers, web-based email)?		
❑ Portable storage devices (e.g., USB sticks, iPods) cannot be connected to endpoint machines and download sensitive data without authorization?		

Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

6. **Evaluate *COSTS vs BENEFITS* of Different Security Methods.**

   Brainstorm different types of security procedures and think about whether they make sense for the type of information you maintain, the format in which it is maintained, the likelihood that someone might try to obtain the information, and the harm that would result if the information was improperly obtained.

7. **Write it Down.**

   Type up the checklists you've just created, the security measures you are taking, and an explanation on why these security measures make sense.

Congratulations – you've just created the foundation of your written security policy!

Minimum Security Checklist for Small Businesses

Minimize What You Save & Store

❑ Don't keep information you don't absolutely need.

❑ Destroy information when it is no longer needed...and destroy it responsibly.

Use Effective Passwords

❑ Never use the default password that may be provided by another company or service provider.

❑ Use "strong" passwords that are *unique to each user.* Strong passwords include some combination of numbers, letters, and symbols. Never use obvious passwords such as your name, your business name, any family member's name, "12345," "ABCDE," "password" or your user name.

❑ Change passwords frequently – every 45-60 days.

Block Potential Intruders

❑ Restrict computer use to business-only purposes. Malware and viruses can sneak onto business machines when employees use them to visit social networking and other personal web sites.

❑ Protect your IT systems from viruses and spyware by using *up-to-date* antivirus protection and firewalls. Most operating systems and antivirus programs contain an automatic update feature that updates the software as new viruses and spyware become known.

❑ Antivirus is not enough. Consider supplementing your antivirus protection and firewalls with other specialized protection tools, such as intrusion prevention and anti-spam technologies.

Back-up and Recover Information

❑ Reduce business downtime from simple human error, hardware malfunctions or disasters. Put protections in place that will ensure your ready access to data and easy data recovery should any of these occur.

Restrict Access

❑ Limit the number of sites/locations where information is stored.

❑ Keep paper records in a locked cabinet, or in a room that stays locked when not in use.

❑ Limit employees' access to data to only those that need the information to do their job.

❑ Take precautions when mailing records. Use a security envelope, require the recipient to sign for the package, and/or ask the delivery service to track the package until it is delivered.

❑ Encrypt sensitive electronic information in every site it is stored.

- Most computer operating systems, including Microsoft's Office, come with basic encryption software already downloaded.
- If you have a business that electronically stores a great deal of sensitive information, invest in higher-level security software to provide advanced encryption software for desktops, laptops, and removable storage devices.
- Do not store sensitive information on portable storage devices (*e.g.*, PDA's, USB drives, CD's, laptops, iPhones, iPods, etc.) as these devices are frequently lost or stolen. If this is unavoidable, make sure the information is encrypted.

❑ Transmit data over the internet using secure connections (*e.g.*, using a Secure Sockets Layer or "SSL" technology). There are several companies that offer relatively inexpensive web-based sites, known as FTPS sites, which can transfer data with a secure connection.

Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Data Security - *Made Simpler*

Sponsored by VISA symantec. KROLL

Additional Resources

❑ **Free Software (trialware)**

✓ Symantec Endpoint Protection Small Business Edition:
www.symantec.com/Vrt/offer?a_id=77956
→ *Sponsor of these BBB materials*

❑ **Causes and impact of losing sensitive electronic data**

http://eval.symantec.com/mktginfo/enterprise/other_resources/b-SMB-Protection-Gap_WP_20094842.en-us.pdf
→ *Sponsor of these BBB materials*

❑ **Techniques to Secure Electronic Data**

✓ Symantec outlines general tips to secure your business from threats
www.symantec.com/business/solutions/smallbusiness/solutiondetail2.jsp?solid=business_owners&solfid=sb_sol_secure_from_threats
→ *Sponsor of these BBB materials*

✓ Podcasts and iTunes – www.symantec.com/podcasts
→ *Sponsor of these BBB materials*

✓ Learn about specialized protection tools, such as Intrusion Prevention and anti-spam technologies, from a Symantec podcast.
→ *Sponsor of these BBB materials*
www.symantec.com/podcasts/detail.jsp?podid=sb_08282009_antivirus

Learn more about Information Back-up tools from a Symantec Webcast.
→ *Sponsor of these BBB materials*
www.symantec.com/offer?a_id=88298

Good practices on how to secure computer systems.
www.onguardonline.gov/topics/computer-security.aspx

✓ Techniques for securing a wireless network
www.onguardonline.gov/topics/wireless-security.aspx

✓ General information concerning encryption
http://computer.howstuffworks.com/encryption.htm

✓ Step-by-step instructions on how to encrypt Microsoft Office documents
http://netsecurity.about.com/od/frequentlyaskedquestions/f/faq_encryptms.htm

✓ Step-by-step instructions on how to encrypt data on a Blackberry device
www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB10916&sliceId=2&docTypeID=DT_SUPPORTISSUE_1_1&dialogID=106798952&stateId=1%200%20106804218

✓ Tips to secure mobile devices and on data security
www.smallbusinesscomputing.com/thebasics/security/

Laws Governing Data Security

Federal Laws

The Gramm-Leach-Bliley Act ("GLBA") and the Health Insurance Portability and Accountability Act ("HIPAA") require that financial and health care providers take steps to ensure that personal information is secure. Consult an attorney to determine if you are covered by these laws, as the government considers many small businesses "financial institutions" or "health care providers" even when the business might not consider itself to be involved in financial services or health care.

State Laws

At least ten states have passed laws requiring small businesses to implement procedures to prevent personal information from being disclosed or improperly used. Some states specifically require that small businesses encrypt personal information that is sent over the Internet. Unlike federal laws, *these state laws apply to all small businesses* – not just those that are financial institutions or a health care provider. Additionally, many states have passed legislation requiring disclosure of any incident involving the loss of consumer information.

Contractual Requirements

Small businesses that accept credit and debit card payments are contractually required to take certain steps to secure the payment card information they collect. Contact the bank or the company that manages your payment card processing for details or visit *http://pcisecuritystandards.org* for more details on the Payment Card Industry Data Security Standard requirements for protecting payment card data.

KELLEY DRYE BRYAN CAVE Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Data Security - *Made Simpler*

Sponsored by VISA symantec. KROLL

❑ **Creating a Data Security Plan.** ***A Snapshot.***

✓ FTC – Fact Sheet on how to create a data security plan.
www.ftc.gov/bcp/edu/pubs/business/idtheft/bus58.pdf

✓ FTC – Interactive Tutorial on creating a data security plan.
www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html

✓ Kroll's Fraud Solutions has an electronic Privacy Training course for organizations and their employees for securing and handling personal information.
www.krollfraudsolutions.com/courses/pa-training/register/standard.aspx
→ *Sponsor of these BBB materials*

❑ **Top Computer Security Risks**

✓ Top 20 security risks listed by the SANS Institute
www.sans.org/top20/

✓ Top 10 security risks listed by e-Security Planet
www.esecurityplanet.com/trends/article.php/1384081/Top-10-Enterprise-Security-Risks.htm

❑ **Providers of Integrated Antivirus and Anti-Phishing Protection, Firewalls Information Back-Up and more.** ***A Snapshot.***

www.symantec.com/business/solutions/index.jsp
→ *Sponsor of these BBB materials*

www.mcafee.com/us/small/index.html

www.zonelabs.com

http://personalfirewall.comodo.com/

www.earthlink.net/software/free/toolbar

http://www.firewallguide.com/freeware.htm

http://us.trendmicro.com/us/home/small-business/?WT.mc_id=2008HP_SB_Tab

www.microsoft.com/security/malwareremove/default.mspx

www.microsoft.com/windows/products/winfamily/defender/default.mspx

www.safer-networking.org/en/index.html

✓ Check a company's BBB Report:
www.bbb.org/us/Find-Business-Reviews

❑ **Providers of SSL certificates – to transmit data securely over the internet.** ***A Snapshot.***

wwww.verisign.com/

www.networksolutions.com/

wwww.thawte.com/

wwww.geotrust.com/

wwww.trustwave.com/

wwww.digicert.com/

✓ Check a company's BBB Report:
www.bbb.org/us/Find-Business-Reviews

❑ **Secure web-based FTP sites for transferring data.** ***A Snapshot***

www.sharefile.com

www.file-works.com

www.ipswitch.com

www.sterlingcommerce.com

https://transport.speedprojects.net/why/default.cfm

www.filesanywhere.com

✓ Check a company's BBB Report:
www.bbb.org/us/Find-Business-Reviews

❑ **Rules for Small Businesses That Accept Payment Cards**

Overview of how to comply with the PCI Data Security Standard.

www.visa.com/cisp
→ *Sponsor of these BBB materials*

www.pcisecuritystandards.org/security_standards/pci_dss.shtml

✓ List of PCI DSS Validated Service Providers

www.visa.com/splisting
→ *Sponsor of these BBB materials*

✓ Check a company's BBB Report:
www.bbb.org/us/Find-Business-Reviews

Before BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Data Security - *Made Simpler*

Sponsored by VISA symantec. KROLL

2. MONITORING & TRANSMITTING FINANCIAL DATA. Do It Securely.

Online banking is a great tool to help small businesses quickly and conveniently track financial information, pay bills, and pay employees. However, data thieves are now targeting small business owners — and their employees — to get access to their online banking credentials and accounts so that they can make unauthorized money transfers. A small business can protect itself against increased liability on its financial transactions by using strong procedures to secure the credentials they use to access their bank accounts.

Getting Started

The following guidelines will help you protect the computers you use to access your bank accounts and your online access credentials.

1. **Initiate a "dual control" payment process with your bank and employees.** Ensure that all payments are initiated from your bank accounts *only after the authorization of two employees.* One employee will authorize the creation of the payment file and a second employee will be responsible for authorizing the release of the file. This process should be in place regardless of the type of payment being initiated… including checks, wire transfers, fund transfers, payroll files, ACH payments, etc.
2. **Have dedicated workstations.** Restrict the use of certain workstations and laptops to be utilized solely for online banking and payments, if possible. For example, a workstation or laptop used for online banking should not be also used for web browsing or social networking.
   - ❑ Lock these workstations when not in use…even for short periods of time.
   - ❑ Do not use public computers — such as at the public library, hotel's Business Center or airport computer terminals — to access online banking.
3. **Use robust authentication methods and vendors.** Make sure your financial service providers allow for "multi-factor authentication." This means that you need more than just a username and password to access your account.

   In addition to passwords and PINs:
   - ❑ Each user should have their own password – *do not have several users share the same password.*
   - ❑ Use 'complex' passwords — ones that contain a combination of numbers, letters and/or symbols.
   - ❑ Consider using an additional authentication tool, such as a token or a smart card.
   - ❑ Each user should change their password frequently – approximately every 45-60 days.
4. **Update virus protection and security software.** Ensure that all anti-spyware, anti-malware, and security software and mechanisms are robust and up-to-date *for all computer workstations and laptops* used for online banking and payments. Implement a process to periodically confirm they remain up-to-date. Security patches are often available via automatic updates.
   - ❑ Do not respond to emails or open attachments…*unless you were expecting the communication.* Phishing scam emails can come from both unrecognized and recognized sources.
   - ❑ *You won't ever receive an authentic email asking for your online banking credentials.*
   - ❑ If something appears unusual or you receive an email requesting your online banking credentials, *call your bank, but don't use any information from the email, as it may be a phishing email.*
5. **Reconcile accounts daily.** Monitor and reconcile accounts daily against expected credits and withdrawals. If you see any kind of unexpected activity on your account, notify your financial institution immediately.
   - ❑ Utilize bank account features, such as automated payment filters and other alerts that show unexpected activity on your accounts.

Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Data Security - *Made Simpler*

Sponsored by VISA symantec. KROLL

3. BECOMING 'PCI COMPLIANT' IF YOU ACCEPT PAYMENT CARDS.

Nearly all businesses today accept credit and debit cards as a form of payment. Because sensitive data is collected in connection with these payments, the payment card industry has developed a comprehensive standard to help ensure the security of cardholder account data. This standard is known as the **Payment Card Industry Data Security Standard** or "PCI DSS," and is managed by the PCI Security Standards Council. The PCI DSS applies to all businesses that store, process or transmit cardholder data, and is enforced by the founding members of the PCI Security Standards Council – Visa Inc., American Express, Discover Financial Services, JCB International, and MasterCard Worldwide.

Getting Started

Ask your merchant bank or third party payment processor to assist you in determining how your business can best comply with the PCI DSS. Data security requirements may vary depending on the type of payment card processing device used, the sophistication level of your payment systems, and the cardholder information you collect and store. For example, businesses that use only imprint machines or standalone dial-out terminals — and do not electronically store cardholder data — need only comply with a subset of the PCI DSS requirements. Businesses using payment systems connected to the Internet or integrated payment applications (i.e., PC-based software applications) must ensure these systems are protected against computer-based attacks.

All businesses that accept credit and debit cards using an integrated payment application and/or e-commerce website should follow these general guidelines.

DO's

See Chapter 1 – Securing Sensitive Data, Additional Resources — for specific guidance.

- ❑ Regularly monitor and test networks/systems that have payment card data.
- ❑ Implement and enforce a company Information Security Policy.
- ❑ Install and keep up-to-date, a firewall that protects cardholder data stored within company systems.
- ❑ Every employee with computer access should be assigned a unique ID and use a robust password (e.g., mix of letters, numbers, and symbols), which is changed frequently (every 45-60 days).
- ❑ Restrict physical access to company systems and records with cardholder data to only those employees with a business "need-to-know."
- ❑ Encrypt cardholder data if transmitting it over wireless or open, public networks.
- ❑ Use and regularly update anti-virus software.
- ❑ Have secure company systems and applications (e.g., good and frequent process to update all computers with necessary patches, process for identifying system/application vulnerabilities, etc.) .
- ❑ Ensure any e-commerce payment solutions are tested to prevent programming vulnerabilities like SQL injection.
- ❑ Use a Payment Application Data Security Standard (PA-DSS) compliant payment application listed on the PCI Security Standards Council website at https://www.pcisecuritystandards.org/security_standards/vpa/.
- ❑ If you outsource the handling of cardholder data to a third party service provider, verify that they have validated PCI DSS compliance and are listed on Visa's website at http://usa.visa.com/merchants/risk_management/cisp_service_providers.html

→ *Sponsor of these BBB materials*

DON'Ts

- ❑ ***Don't store*** magnetic stripe cardholder data or the CVV2 code (the three digit value on the back of Visa cards) after ***authorization***.
- ❑ ***Don't use*** vendor-supplied or default system passwords or common/weak passwords.
- ❑ ***Don't store*** cardholder data in any systems in clear text.
- ❑ ***Don't leave*** remote access applications in an "always on" mode.

KELLEY DRYE BRYAN CAVE Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Additional Resources

For additional information on the PCI DSS and how it relates to your credit or debit card acceptance, contact your merchant bank or third-party payment processor. Many merchant banks and third-party payment processors may require their merchants to demonstrate compliance with the PCI DSS through an approved security vendor program.

- ❑ PCI Security Standards Council website: www.pcisecuritystandards.org/index.shtml.
- ❑ Visa Data Security website: www.visa.com/cisp.
  → *Sponsor of these BBB materials*

Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Data Security - *Made Simpler*

Sponsored by VISA symantec. KROLL

4. DISPOSING OF DATA. Do It Responsibly.

It is generally a good idea to make sure that any document, whether it is a paper document or an electronic document, is completely destroyed when you no longer need it if it contains information about you or your business, any of your customers, potential customers, or employees. Here are some general and easy-to-follow guidelines.

Destroying Paper Records Yourself

- ❑ Shred all sensitive paper documents. *Never just deposit them in the trash or dumpster.*
- ❑ Ideally, use a shredder that cross-cuts, confetti-cuts, or particle-cuts.
- ❑ For extremely sensitive information use a "disintegrator," "granulator," "hammermill" or "grinder." These devices tear paper at random, or tear paper into extremely small pieces.

Destroying Electronic Records Yourself

What Works

- ❑ Use data wiping software. It removes information by writing new, meaningless information on top of old information.
- ❑ Shred CDs and DVDs.
- ❑ "Magnetically degauss" hard drives in old computers. Magnetic degaussing uses extremely strong magnets to remove the magnetic encoding that stores data. Although degaussing machines are expensive, many companies charge less than $10 to degauss a hard drive.

What Does Not Work

- ❑ *Breaking an old computer.* Breaking an old computer does not mean that you are breaking the media where data is stored (e.g., the hard drive). Although it is possible to remove the hard drive and then physically destroy it (e.g., drilling a hole through it) this can be time-consuming and dangerous if you don't have the right equipment.
- ❑ *Microwaving CDs and DVDs.* Although microwaving a CD or DVD destroys the data on the CD or DVD, it may also release toxic fumes into your microwave or cause a fire.
- ❑ *Placing it in the "Recycle Bin" on your desktop, or clicking "Delete."* It may disappear from your screen, but it still exists and could be recovered by a computer expert.

Hiring a Company

- ❑ Consider using a certified disposal company. The National Association for Information Destruction (NAID) audits their member companies for compliance with the association's standards.
- ❑ Ask if they have been independently audited or certified, and request a copy of the audit or certification.
- ❑ Check the company's BBB Report at www.bbb.org.
- ❑ Ask for several references and call the references.
- ❑ Ask for a signed agreement that explains the company's procedures for destroying documents.

Additional Resources

- ❑ **Paper Shredders**
  Description of different types of paper shredders.
  http://en.wikipedia.org/wiki/Paper_shredder

- ❑ **Free Data Wiping Software – A Snapshot**
  - ✓DBAN
    www.dban.org
  - ✓Active @ KillDisk
    www.killdisk.com
  - ✓Check a company's BBB Report:
    www.bbb.org/us/Find-Business Reviews

Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Data Security - *Made Simpler*

Sponsored by VISA symantec. KROLL

❑ **Methods for Physically Destroying Electronic Media**

- ✓ Explanation of methods for destroying a CD/DVD. www.wikihow.com/Destroy-a-CD-or-DVD
- ✓ Video explaining 4 methods for destroying a hard drive. www.ehow.com/video_4992405_destroy-hard-drive.html

❑ **Businesses Providing Degaussing or Hard Drive Shredding – A Snapshot**

- ✓ Security Engineered Machinery Co. www.semshred.com/content291.html
- ✓ Garner Products www.garner-products.com/Degserv.htm
- ✓ Check a company's BBB Report: www.bbb.org/us/Find-Business-Reviews

❑ **Free software (Trialware)**

- ✓ Symantec Endpoint Protection Small Business Edition www.symantec.com/Vrt/offer?a_id=77956
  → *Sponsor of these BBB materials*
- ✓ Symantec Brightmail gateway www.symantec.com/Vrt/offer?a_id=65009
  → *Sponsor of these BBB materials*

❑ **Find an Information Destruction Provider in your Area**

- ✓ List of NAID certified document destruction providers www.naidonline.org/members.html
- ✓ Check a company's BBB Report: www.bbb.org/us/Find-Business-Reviews

Laws Governing Data Disposal

Federal Laws

The Fair Credit Reporting Act (FCRA) and the Federal Trade Commission's Rule concerning the Disposal of Consumer Report Information and Records (the Disposal Rule) requires small businesses that obtain consumer information from consumer reporting companies (e.g., Equifax, Experian, or TransUnion) to take "reasonable measures" to properly dispose of that information. Health care providers and financial institutions may have additional obligations to destroy consumer information under the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA).

State Laws

Approximately 19 states have statutes that require small businesses to dispose of records that contain personal information. Similar to the Disposal Rule, the majority of these statutes require small businesses to take "reasonable steps" when destroying records. Some of the state statutes only apply to specific types of small businesses, such as health care providers, financial institutions, or tax preparers. You should consult an attorney to determine whether any state laws apply to your business.

FTC Disposal Rule

www.ftc.gov/os/2004/11/041118disposalfrn.pdf

HIPAA Rules

www.cms.hhs.gov/HIPAAGenInfo/Downloads/HIPAALaw.pdf

GLBA

http://straylight.law.cornell.edu/uscode/html/uscode15/usc_sup_01_15_10_94.html

KELLEY DRYE BRYAN CAVE Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Data Security - *Made Simpler*

Sponsored by VISA symantec. KROLL

5. COMMUNICATING YOUR DATA SECURITY PROGRAM TO YOUR CUSTOMERS

Telling your customers that you have a data security policy in place will both build their trust and differentiate you from your competitors.

Only 28% of US small businesses have a formal Internet security policy.

Source: 2009 National Small Business Study, National Cyber Security Alliance & Symantec.

Getting Started

There is a sensible line to walk when communicating your data security plan. You need to

a) Decide how much you communicate (too much detail will help criminals);

b) Ensure your communication is accurate, and

c) Put what you preach into action on an ongoing basis.

1. Information to Share.

- ❑ Obtain a third-party seal that verifies your small business uses an appropriate level of security to protect your website, or your Internet transactions. This can be a visual tool to communicate to customers that you have qualfied for a level of certification – which is something customers are actively looking for more and more.
- ❑ Make sure that whatever information you communicate to your customers that you do...You Do!...and is up-to-date. For example, if you tell consumers that you keep their information on computers that you own, and later contract with another company to provide off-site computer storage space, make sure that you reflect your new practices in your public policies.
- ❑ Tell customers what you will do in the event that you discover that their information has been lost or stolen. *For more detail, see Chapter 7 "If Customer Data is Lost or Stolen. What To Do Next."*

2. Information NOT to Share.

- ❑ DO NOT share detailed information about your security systems. Remember, criminals see what your customers see, and they can use public information about your security systems to evade them (e.g., the encryption software you use, or where you store documents).
- ❑ DO NOT tell customers that there is no risk of ID Theft, or that their information is "100% safe." No matter how hard you try to protect customer information, there is always a chance that someone may obtain and misuse it.
- ❑ DO NOT guarantee or promise that a customers' information can never be lost or stolen unless you tell customers what you will do if that promise is broken.

Additional Resources

❑ **Companies that Validate Safety of Web sites or Provide Online Data Security Seals of Approval.** ***A Snapshot***

- ✓ Symantec
  http://safeweb.norton.com/dirtysites
  → *Sponsor of these BBB materials*
- ✓ Trust Guard
  www.trust-guard.com
- ✓ Web Entrust
  www.webentrust.com/trusted.html
- ✓ Control Scan
  www.controlscan.com
- ✓ McAfee
  www.mcafeesecure.com/us
- ✓ Comodo
  www.comodo.com/hackerproof
- ✓ Check a company's BBB Report:
  www.bbb.org/us/Find-Business-Reviews

Legal Requirements

Generally small businesses are not required under federal or state law to make public how they protect information.

If a small business chooses to publish information concerning how it protects the sensitive personal information that it keeps, how it spots identity theft, how it responds when data is lost or stolen, or how it disposes of data the Federal Trade Commission Act and consumer protection statutes in almost every state and territory prohibit the small business from making false or deceptive statements.

KELLEY DRYE BRYAN CAVE Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Data Security - *Made Simpler*

Sponsored by VISA symantec. KROLL

6. SPOTTING IDENTITY THEFT

Identity theft can take many different forms. For example, a criminal might try to use another person's name and address when establishing an account with a small business that offers delayed (30-days) billing after the date of sale. Or a criminal might try to log-in to another customer's account and make transactions without their authorization. Or another might use a stolen credit card number to buy products and services.

Only 35% of small businesses provide training to employees about Internet safety and security.

Source: 2009 National Small Business Study

Getting Started

For a small business, combating identity theft is a three-step process, *which needs to be put into motion before an event occurs:*

1. **Identify Types of Suspicious Behavior.** Identify *in advance* what constitutes suspicious behavior. This is often referred to as the "red flags" of identity theft. Although red flags differ between businesses and between industries, the following types of red flags are common to most small businesses:
   - ❑ A customer reports that they have seen suspicious activity in one of their accounts.
   - ❑ A customer opens a new account that contains suspicious elements.
   - ❑ A customer presents you with suspicious documents (e.g., altered ID card, different addresses on different forms of ID, a PO Box as a home address).
   - ❑ You (or your employees) notice unusual activity relating to a customer's account.
2. **Develop Policies To Detect Suspicious Events Early — & Train Your Employees.** Put policies into place that will help you and your employees identify a red flag and catch suspicious events early...or even as they occur. Policies will differ depending on your business and your industry, but the following are examples of ways you can train your employees, which will become the basis for your Red Flag Detection policy:
   - ❑ Train about types of red flags they might see when a customer opens an account.
   - ❑ Train about types of red flags they might see when a customer orders a product/service.
   - ❑ Train about types of red flags they might see on an existing account.
3. **Respond to Suspicious Behavior.** Detecting red flags needs to be matched with potential action plans. The type of action will depend on the type of red flag...and the risk that red flag could lead to identity theft. Here are some possible action plans, depending on the circumstances:
   - ❑ Report the red flag event to the police or to other law enforcement agencies, such as the Federal Trade Commission or your state attorney general's office.
   - ❑ If the red flag involves Internet sales you can report the event on-line with the FBI's Internet Crime Complaint Center www.ic3.gov/default.aspx.
   - ❑ Alert your customer that suspicious behavior has been observed on their account.
   - ❑ Refuse to complete a transaction until the suspicious event can be explained.
   - ❑ Request that your customer provide additional documentation to verify that they are who they say they are.
   - ❑ Request that your customer explain the suspicious activity.
4. **Write It Down.** Type up the lists you just created, above: 1) The red flags that could affect your small business, 2) The ways in which your small business will detect suspicious events, and 3) How your business will respond to suspicious behavior.

Congratulations — you've just formed the foundation of your Red Flags Policy.

- ❑ Update your policy periodically — at least once a year.
- ❑ Share your policy with all of your employees, and use it to help train them on how to detect and respond to identity theft.

KELLEY DRYE BRYAN CAVE Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Additional Resources

❑ **Do-It-Yourself ID Theft Policies**

✓ The FTC has provided a Do-It-Yourself form for businesses that are at low-risk of identity theft.

www.ftc.gov/bcp/edu/microsites/redflagsrule/RedFlags_forLowRiskBusinesses.pdf

❑ **Risk Consulting Companies. *A Snapshot***

✓ Kroll's Fraud Solutions has created several resources to understand the risks of identity theft, both for businesses and consumers. Resources include white papers on identity theft awareness and avoidance, as well as a glossary on identity theft terms.

www.krollfraudsolutions.com/understanding-id-theft.

→ *Sponsor of these BBB materials*

❑ **Complying with FTC Red Flags Policy**

✓ FTC, Fighting Fraud with the Red Flags Rule, a How-To Guide for Business

www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf

✓ FTC interpretation of Red Flags Rule

www.ftc.gov/bcp/edu/microsites/redflagsrule/more-about-red-flags.shtm

✓ Kroll's Fraud Solutions has created an electronic Employee Training course entitled "Red Flags Rule: Identify, Detect, Respond" to assist affected organizations comply with the Red Flags Rule

www.krollfraudsolutions.com/understanding-id-theft/red-flag-rules.aspx

www.krollfraudsolutions.com/courses/pa-training/register/red-flag-rules.aspx

→ *Sponsor of these BBB materials*

Legal Requirements

The Fair and Accurate Transactions Act ("FACTA") requires "financial institutions" and "creditors" that maintain accounts for their customers to create a written program to detect, prevent, and mitigate identity theft.

Although you may not think that your business is a "financial institution" or is a "creditor," the Federal Trade Commission considers any business that allows customers to defer payment when they receive goods or services to be a creditor. This includes all small businesses which bill customers after providing services.

The Federal Trade Commission has published a legal rule, called the Red Flags Rule, to provide small businesses with guidance concerning how to comply with FACTA.

You should consider consulting an attorney to determine if you are covered by FACTA, if you are required to have a written program (a "Red Flags Policy"), and whether your Red Flags Policy complies with the Red Flags Rule.

You should also consider collaborating with a risk consulting company to help identify, detect, and respond to red flags.

Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Data Security - *Made Simpler*

Sponsored by VISA symantec. KROLL

7. IF CUSTOMER DATA IS STOLEN OR LOST. What To Do Next.

A small business must respond quickly if sensitive customer information is lost or stolen, giving an unauthorized person access to that sensitive information. If this occurs, you'll need to notify the affected customers.

85% of data breaches occur at the small business level.

Source: Visa

Getting Started

1. **Create a Data Breach Notification Policy.** A data breach notification policy tells consumers how your small business will notify its customers if a data breach occurs.

❑ Consider informing consumers that you will notify them through a quicker and relatively inexpensive method (e.g., email or publication) instead of a more expensive method (e.g., US mail). However, there are state-specific laws on the notification delivery method, so consult with an attorney before sending out any notices.

2. **Train Your Employees to Identify Breaches.** Employees need to know how to spot a potential breach and how to report this type of event. Consider the following points for your employee training:

❑ Teach employees what constitutes a "data breach." This might include:

- Inadvertently sending information to the wrong person via mail or email.

❑ Instruct employees to report any event where personal information is accessed or acquired by an unauthorized person *to you or to a specific supervisor.*

❑ Consider providing employees a confidential means of reporting a data breach. This can be particularly useful if your employees might be afraid that reporting a data breach might result in negative actions against them or one of their colleagues.

3. **Immediately Gather the Facts of a Potential Breach.**

❑ Investigate the basic facts surrounding the incident.

❑ Keep a written chronology of what you learn, when you learned it, and from whom.

❑ If your business is short on internal resources, consider obtaining the assistance and guidance of a data forensic expert to assist in your investigation.

❑ Your investigation should try to answer the following questions:

- *Was the data kept on paper or in an electronic record?*
- *If the data was kept electronically, was it encrypted?*
- *Did the data include names and/or addresses?*
- *Did the data include any financial account numbers or payment card numbers?*
- *Did the data include any birth dates?*
- *Did the data include any Social Security Numbers?*
- *Did the data include any other information that could be linked to specific consumers?*
- *How many people's information was included?*
- *Did the affected individuals include children?*
- *In what states did the affected people reside?*
- *In what countries did the affected people reside, and what languages do they speak?*

KELLEY DRYE BRYAN CAVE Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Data Security - *Made Simpler*

Sponsored by VISA symantec. KROLL

4. **Notify Financial Institutions.** If financial information, such as payment card numbers, was compromised, contact the bank or company that manages your payment card processing.

5. **Seek Outside Counsel.** Seek attorney assistance or guidance from a risk consulting company as soon as you become aware of an incident that might constitute a data security breach. Your attorney can help you identify which laws might be involved, and whether you need to alert consumers or the government of the incident. Consider asking the following questions to the outside counsel you engage:

   ❑ *Which state laws apply to the incident?*

   ❑ *Would the incident be considered a "data security breach" under those laws?*

   ❑ *Am I required to notify consumers of the incident?*

   ❑ *Am I required to notify the government of the incident?*

   ❑ *If so, which government agencies must be notified?*

   ❑ *If not, should I voluntarily notify my local law enforcement, or the FBI?*

   ❑ *Am I required to notify the consumer reporting agencies (e.g., Experian, Equifax, and TransUnion)?*

   ❑ *Am I required to notify the payment card companies of the incident?*

   ❑ *If notification is required, how much time do I have to issue those notices?*

   ❑ *What is required if the affected individuals live abroad?*

   ❑ *What information is required in the notification letter?*

   ❑ *How and in what format should the notification letter be sent?*

6. **Notify Affected Customers.** Notify them in the manner you said you would in your Data Security Policy.

   Advise them of:

   ❑ *What occurred*

   ❑ *When it occurred*

   ❑ *The specific steps you are taking to address the event*

Additional Resources

❑ **Free Templates**

✓ Sample letter provided by the FTC
www.ftc.gov/bcp/edu/microsites/idtheft/downloads/model-letter.doc

❑ **What To Do If Compromised?**

✓ http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html.

→ *Sponsor of these BBB materials*

Legal Requirements

Federal Laws

The Gramm-Leach-Bliley Act ("GLBA") and the American Recovery and Reinvestment Act require that certain financial institutions as well as health care providers, or businesses that provide services to health care providers, notify patients and the government if the security of the personal information that they maintain is breached.

You should consult an attorney to determine if you are covered by one of these statutes.

State Laws

Almost every state and territory, including the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, has enacted a "data breach notification" statute. Although statutes vary between states, data breach notification statutes generally require businesses that have personal information about residents within a state to notify those residents if someone who is not authorized acquires that information.

You should consult an attorney to determine which state data breach notification statutes apply to your business, and what the specific requirements of those statutes might be.

GLBA Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.
www.occ.treas.gov/consumer/Customernoticeguidance.pdf

Links to state data breach notification statutes
www.ncsl.org/Default.aspx?TabId=13489

Summary of federal state data breach and privacy statutes
www.krollfraudsolutions.com/understanding-id-theft/legislation-identity-fraud.aspx

Summary of state data breach notification statutes
www.consumersunion.org/campaigns//financialprivacynow/002215indiv.html

KELLEY DRYE BRYAN CAVE Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Data Security - *Made Simpler*

Sponsored by VISA symantec. KROLL

❑ **Information Concerning Past Data Breaches**

✓ Chronological list maintained by Privacy Rights Clearinghouse www.privacyrights.org/ar/ChronDataBreaches.htm

❑ **Risk Consulting and Data Forensics Companies – *A Snapshot***

✓ Identity Theft Response and Recovery Services www.krollfraudsolutions.com/breach-products-and-services/data-breach-recovery.aspx

→ *Sponsor of these BBB materials*

❑ **Minimizing Cost of Data Breach**

✓ Article - "Ten Ways to Prevent a Data Breach from Breaching a Budget." www.bryancave.com/files/upload/zetoony.pdf

✓ Article - "How to Minimize the Impact of a Data Security Breach" www.csoonline.com/article/451785/How_to_Minimize_the_Impact_of_a_Data_Breach

❑ **Information On How to Contact Credit Reporting Agencies**

✓ FTC guidance on responding to data breach including contact information for credit reporting agencies. www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html

✓ Equifax www.equifax.com/help/data-breach-solutions/

✓ Experian (Data Breach Support) www.experian.com/customer_service/contact_business.html

✓ TransUnion (Data Breach Hotline) www.transunion.com/corporate/business/clientSupport/contactUs.page

✓ Check a company's BBB Report: www.bbb.org/us/Find-Business-Reviews

❑ **Companies That Can Assist in Notifying Consumers of Data Breach – *A Snapshot***

✓ Kroll's Fraud Solutions www.krollfraudsolutions.com/breach-product-and-services/data-breach-recovery.aspx

→ *Sponsor of these BBB materials*

✓ Experian www.experian.com/credit_solutions/fraud/avert.html?sc=668948bcd=semidtgsm090415ch85

✓ Equifax www.equifax.com/help/data-breach-solutions2/?CMP=KNC-Google&HBX_PK=data_breach&HBX_OU=50

KELLEY DRYE BRYAN CAVE Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Data Security - *Made Simpler*

Sponsored by VISA symantec. KROLL

8. GLOBAL ENTERPRISES. Data Security Issues to Consider.

Data security laws and regulations differ dramatically between countries. Small businesses doing business outside of the United States should consult their attorney to determine what, if any, foreign requirements exist concerning how to treat data that you obtain abroad.

Getting Started

Because of the differences in data security standards, laws, and practices from country to country, you should consult with an attorney that is familiar with the laws of each of the foreign countries in which you do business. When talking to your attorney consider asking the following questions:

- ❑ *What types of information are protected in the foreign country?*
- ❑ *Are there any restrictions on how information can be collected in the foreign country?*
- ❑ *Are there any restrictions on how information must be stored in the foreign country?*
- ❑ *Are there any restrictions on how information can be used in the foreign country?*
- ❑ *Are there any laws limiting how long information can be stored once it is collected?*
- ❑ *Can information collected by my business in the foreign country be transferred to the United States, or does it have to be stored and used in that country?*
- ❑ *If I transfer information to the United States, am I restricted from providing that information to other parties, such as companies that assist my business with administrative support?*
- ❑ *Do any restrictions apply to information that I maintain about employees that I hire in foreign countries?*

Additional Resources

Laws and Regulations of Foreign Countries

- ✓ European Commission website on data privacy and protection. http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm
- ✓ List of statutes in foreign countries that might relate to data security. www.searchinfo.com/services/DPL.pdf
- ✓ List of privacy related statutes by country www.mofoprivacy.com/default.aspx?tabNum=2
- ✓ US-European Union Safe Harbor Framework
  US Department of Commerce website listing US companies eligible to receive personal data from the EU. http://www.export.gov/safeharbor/eu/index.asp
- ✓ BBB EU Safe Harbor dispute resolution program for member companies of the US-EU Safe Harbor. http://www.bbb.org/us/european-union-dispute-resolution/

Legal Requirements

Different countries take extremely different approaches to data security.

For example, the European Union considers ***any*** information relating to an identified person to be protected "personal information."

Among other things, the European Union severely restricts companies from transferring personal information from the European Union to countries, like the United States, that the European Union considers to have inadequate data protection laws.

As a result, a small business may have to take special steps to transfer personal information from the European Union to the United States – even if that information is being transferred within the small business.

KELLEY DRYE BRYAN CAVE Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Data Security - *Made Simpler*

Sponsored by VISA symantec. KROLL

9. IF THIRD-PARTIES REQUEST YOUR DATA. How To Respond.

Before providing any consumer information to a third-party you should make sure that they are actually authorized to have that information.

Getting Started

Here are some guidelines to help you — and your employees — determine who is — *and who is not* — authorized to obtain personal information about your customers.

Requests From Your Customers

In general, customers are authorized to find out what information you keep about them.

Requests from Individuals Connected with Your Customers

❑ *If your customer indicates that he/she wants someone else to see the information* that you keep about the customer, consider that third-party as now "authorized."

❑ However...if you receive *a request from a third-party for information about your customer...*consider:

- Requiring written authorization. If a third party such as a family member, an attorney, or a health care provider requests information, require the third-party to provide you with written authorization (e.g., a consent form, or a power-of-attorney) which has been signed and notarized by the individual.
- Carefully read the written authorization and make sure that it encompasses the type of information that you plan to disclose.

Requests from the Government

If you receive a request from your state or the federal government to obtain personal information about your customers, and your customers have not consented to that request, **consult your attorney**. Consider the following:

❑ *Don't assume that a government request is "authorized."* Just because a request comes from the government does not mean that the government is "authorized" to obtain personal information.

❑ Try to comply with the request without providing personal information. Sometimes government agencies request documents that include personal information without realizing it.

❑ If you and your attorney decide to comply with a government request, consider asking the government if you can delete the personal information that may be in the document.

Requests from Other People

❑ *Other people, companies, or organizations that request personal information* about your customers are generally not considered "authorized." Consider:

- Requiring a formal request – in writing.
- Consult with your attorney.
- After consulting with your attorney, and/or the customer, respond to the request in writing and keep a copy of your response.

❑ *If you receive a subpoena from an attorney,* **do not assume that the request is "authorized."**

- The mere fact that someone issues a subpoena *does not* mean that you must provide them with the information that they request.
- Immediately consult your attorney who can help you decide how to respond to the subpoena.

Legal Requirements

Federal and state laws require businesses to take steps to prevent personal information from being obtained by "unauthorized" individuals, and to alert consumers, and the government, if "unauthorized" individuals access and/or acquire that information.

As a result, businesses must ensure that they only release information to "authorized" third parties.

Responding to Subpoenas
www.citmedialaw.org/legal-guide/responding-subpoenas

KELLEY DRYE BRYAN CAVE Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

10. COMMON TECHNICAL AND LEGAL TERMS[1]

The terms can be confusing. The following glossary may help you understand some of the legal, technical, and industry terms that are often used when discussing data security.

[1]Many, but not all, of the terms and definitions listed were compiled by the FTC. www.onguardonline.gov/tools/learn-terms.aspx.

TERM	EXPLANATION
Adware	A type of software that often comes with free downloads. Some adware displays ads on your computer, while some monitors your computer use (including websites visited) and displays targeted ads based on your use.
Anti-virus Software	Protects your computer from viruses that can destroy your data, slow your computer's performance, cause a crash, or even allow spammers to send email through your account.
Bookmark	A web browser feature that allows you to save the addresses of interesting or frequently used websites, so that you can readily revisit them.
Broadband	A number of different methods used for high speed Internet access such as DSL, cable modems, fiber optics, and mobile wireless, all of which are permanently connected to the Internet through different means.
Browser Hijacker	A common spyware program that changes your web browser's home page without the user's knowledge, even if you change it back.
Cache	A form of computer memory that allows you to access stored information, such as web addresses you've recently typed into your browser, more quickly. Pronounced "cash."
Cookies	A small text file that a website can place on your computer's hard drive to collect information about your activities on the site or to allow the site to remember information about you and your activities.
Data Security Incident	A situation in which you believe that electronic data that contains Personally Identifiable Information ("PII") may have been improperly accessed or acquired....which compromises the security, confidentiality or integrity of "PII" maintained by a business.
DOB	Date of birth.
Domain	A segment of Internet space, denoted by the function or type of information it includes; current domains include ".com" for commercial sites, ".gov" for governmental ones, and ".org" for non-commercial organizations.
Drive-by Download	Software that installs on your computer without your knowledge when you visit certain websites. To avoid drive-by downloads, make sure to update your operating system and Web browser regularly.

cont.

KELLEY DRYE BRYAN CAVE Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

TERM	EXPLANATION
DSL	Digital Subscriber Line: A type of high speed Internet using standard phone lines and the local network. DSL is almost always slower than cable modem or fiber optics.
Encryption	The scrambling of data into a secret code that can be read only by software set to decode the information.
Endpoint	Any computer — desktop, laptop, or server.
Extended Service Set Identifier (ESSID)	The name a manufacturer assigns to a router. It may be a standard, default name assigned by the manufacturer to all hardware of that model. Users can improve security by changing to a unique name. Similar to a Service Set Identifier (SSID).
Filter	Software that screens information on the Internet, classifies its content, and allows the user to block certain kinds of content.
Firewall	Hardware or software that helps keep hackers from using your computer to send out your personal information without your permission. Firewalls watch for outside attempts to access your system and block communications to and from sources you don't permit.
FTC	The Federal Trade Commission. *See* www.ftc.gov.
GLBA	The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act. Pub. L. 106-102, codified at 15 U.S.C. §§ 6801-6809 and §§ 6821-6827 as amended. A full copy of the Act is available at http://straylight.law.cornell.edu/uscode/html/uscode15/usc_sup_01_15_10_94.html
Hacker	Someone who uses computers and the Internet to access other people's computers without permission.
Hardware	The mechanical parts of a computer system, including the central processing unit (CPU), monitor, keyboard, and mouse, as well as other equipment like printers and speakers.
HIPAA	The Health Insurance Portability and Accountability Act. Pub. L. 104-191, 110 Stat. 1936, codified at 29 U.S.C. §§ 1181, 1320, 1395. A full copy of the Act is available at www.cms.hhs.gov/HIPAAGenInfo/Downloads/HIPAALaw.pdf
HTTP (Hypertext Transfer Protocol)	The standard language that computers connected to the World Wide Web use to communicate with each other.
Internet	The computer language that allows computer programs
Protocol (IP)	to communicate over the Internet.
IP Address	A computer's "address," it consists of a series of numbers separated by periods.
Keystroke Logger	A device or program that records each keystroke typed on a particular computer.
LAN (Local Area Network)	A network of connected computers that are generally located near each other, such as in an office or company.
Malware	A combination of the terms "malicious" and "software," used to describe any software designed to 'infect' a single computer, server, or computer network. Malware includes malicious software, such as viruses, Trojans, key loggers, spyware, etc – programs used to steal sensitive data. Once in your computer, they can steal information, send spam, and commit fraud.

cont.

KELLEY DRYE BRYAN CAVE Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

TERM	EXPLANATION
Media Access Control (MAC) Address	A unique number that the manufacturer assigns to each computer or other device in a network.
Monitoring Software	Programs that allow a parent or caregiver to monitor the websites a child visits or email messages he or she reads, without blocking access.
Network	A group of two or more computers that are able to communicate with one another.
Online Banking Credentials	The unique identification used by consumers when they are accessing systems that transmit financial data. These credentials often include, but are not limited to, a username, password, smart card, token, or a biometric.
Online Profiling	Compiling information about consumers' preferences and interests by tracking their online movements and actions in order to create targeted ads.
Operating System	The main program that runs on a computer. An operating system allows other software to run and prevents unauthorized users from accessing the system. Major operating systems include UNIX, Windows, MacOS, and Linux.
P2P, Peer-to-Peer	A method of sharing files, usually music, games, or software with other users through a sharing program that allows uploading and downloading files from other users online. Caution should be used — P2P files are often misrepresented and can contain offensive material, malware, viruses, or other unintended items.
PCI	The term "PCI" stands for Payment Card Industry.
PCI Data Security Standard	This refers to a data security standard promulgated by members of the payment card industry. Additional information about the PCI Data Security Standard can be found at www.visa.com/cisp.
Personal Digital Assistance (PDA)	A handheld device that combines various forms of traditional computer and telecommunications products. Common examples include Blackberrys, and iPhones.
Personal Information	Information that can identify you, like your bank and credit card account numbers; your Social Security Number (SSN); or your name, address, phone numbers, email addresses, or date of birth.
Phishing	A scam that involves Internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims.
RAM	Short-hand for "Random Access Memory," it's the hardware inside your computer that retains memory on a short-term basis and stores information while you work.
Router	A device that connects two or more networks. A router finds the best path for forwarding information across the networks.
Secure Socket Layer (SSL)	A protocol developed for transmitting private documents via the Internet.
Sock Puppet	A secret alias used by a member of an Internet community, but not acknowledged by that person.

cont.

KELLEY DRYE BRYAN CAVE Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

Data Security - *Made Simpler*

Sponsored by VISA symantec. KROLL

TERM	EXPLANATION
Software	A computer program with instructions that enable the computer hardware to work. System software — such as Windows or MacOS — operate the machine itself, and applications software — such as spreadsheet or word processing programs — provide specific functionality.
Spam	Unsolicited commercial email, often sent in bulk quantities.
Spam Zombies	Home computers that have been taken over by spammers without the consent or knowledge of the computer owner. The computers are then used to send spam in a way that hides the true origin.
Spammer	Someone who sends unsolicited commercial email, often in bulk quantities.
Spyware	A software program that may be installed on your computer without your consent to monitor your use, send pop-up ads, redirect your computer to certain websites, or record keystrokes, which could lead to identity theft.
Trojans	Programs that, when installed on your computer, enable unauthorized people to access it and sometimes to send spam from it.
Universal Serial Bus (USB)	A connection standard that allows data to be transferred between a computer and a peripheral device such as a mouse, a keyboard, or an external hard drive. The USB port, has largely replaced the serial port and the parallel port found on older products.
Virus	A program that can sneak onto your computer — often through an email attachment — and then make copies of itself, quickly using up all available memory.
Wi-Fi Protected Access (WPA)	A security protocol developed to fix flaws in WEP. Encrypts data sent to and from wireless devices within a network.
Wired Equivalent Privacy (WEP)	A security protocol that encrypts data sent to and from wireless devices within a network. Not as strong as WPA encryption.
Wireless Network	A method of accessing high speed Internet without the computer being linked by cables.
Worm	A program that reproduces itself over a network and can use up your computer's resources and possibly shut your system down.

Additional Resources

- ❑ Glossary of Key Information Security Terms Published by the National Institute of Standards and Technology
  http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf
- ❑ Glossary of Terms Used in Security and Intrusion Detection published by SANS.org
  www.sans.org/resources/glossary.php
- ❑ Online dictionary and search engine for computer and internet technology terms
  www.webopedia.com
- ❑ Glossary by Kroll's Fraud Solutions, which contain the most common words involving data security and information protection relating specifically to identity theft, fraud, checking, credit and non-credit data.
  www.krollfraudsolutions.com/understanding-id-theft/glossary.aspx

The resources in *Data Security Made Simpler* do not constitute an exhaustive list of all data security products and services available. As a matter of policy, BBB does not endorse any product, service or business. Readers are advised to investigate before buying and especially to check at bbb.org for a business' current BBB Reliability Report.

KELLEY DRYE BRYAN CAVE Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

11. ABOUT OUR TOPIC EXPERTS

Dana B. Rosenfeld, Kelley Drye LLP

Dana Rosenfeld has served as the Assistant Director of the Federal Trade Commission's Bureau of Consumer Protection, and as an advisor to the former Chairman of the Federal Trade Commission, Robert Pitofsky, and the former Director of Consumer Protection, Jodie Bernstein.

drosenfeld@kelleydrye.com
www.kelleydrye.com/attorneys/atty_data/06163

KELLEY DRYE

David A. Zetoony, Bryan Cave LLP

David Zetoony has served as a consumer protection liaison and vice-chair to the American Bar Association's Antitrust Telecommunications and Health Care and Pharmaceutical Industry Committees. Zetoony has counseled dozens of companies on how to respond to data security breaches and has written numerous articles on the subject.

David.Zetoony@bryancave.com
www.bryancave.com/davidzetoony/

BRYAN CAVE

Data Security - *Made Simpler*

Sponsored by VISA symantec. KROLL

Frequently Asked Questions

Given all the things I need to juggle to run my business, why should I make Data Security a priority?

One word — ***"Trust."*** As hard as you've worked to earn your customers' trust in you and your business, it can take just one trigger to break that trust. *Your ability to keep your customers' sensitive data secure is one of those make-it-or-break-it triggers.* Customers expect that every business — large or small — that collects their sensitive personal information will protect it. Beyond customer expectations, there's the law. Depending on your type of business and the states in which your customers reside, you may be legally required to protect the personal information you collect.

This feels overwhelming. How do I even start this process?

It will be less overwhelming if you approach this piece by piece. First — determine what makes sense for your type of business. This will be based on the type of data that you collect and store,and the kind of resources you have managing that data.

If your small business keeps information about customers in several formats (e.g., on paper, on computers, and online), you should sit down with a team of your employees and discuss these issues together to make sure you consider all viewpoints.

1. *Inventory all your data and its various types and forms.*
2. *Inventory all the different sites where you store data.*
3. *Inventory potential sources for data leaks.*
4. *Evaluate the costs versus benefits of different security methods.*
5. *Write this all down,* and you'll have just created the foundation of your written security policy!

Refer to Chapter 1 of "Data Security — *Made Simpler*" for some useful checklists that will make this process easier for you and your team.

What are four (4) minimum things a small business should be doing for data security?

1. If you don't need it, don't collect it...and don't store it. If you have it and don't need it any more, destroy it — responsibly.
2. *Restrict and limit access — by — to sensitive data.* Use locks on doors and file cabinets. Limit employee access to data to those that need it to do their jobs. Take precautions when mailing records. Encrypt sensitive electronic information in every site it is stored — on computers; On laptops On PDAs, iPhones and iPods; On USB drives (sometimes called "thumb" drives"). Transmit data over the internet using secure connections (SSL technology).
3. *Use effective passwords...and issue a unique password to every employee.* Never use the default password that comes from another product or service provider. Never use obvious passwords, such as your name, business name, family member's name, "12345," "ABCDE," "password," or your user name. Change passwords every 45-60 days.
4. *Block potential intruders.* Protect your IT systems from viruses and spyware by using antivirus protection and firewalls. Make sure these protections are up-to-date.

Refer to Chapter 1 of "Data Security — *Made Simpler*" for more information on these four guidelines and potential resources to help.

KELLEY DRYE BRYAN CAVE Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

What's the best way to destroy paper documents?

Shred them yourself, or hire a reputable shredding company to do it for you. *Never just toss paper documents containing sensitive information in the trash or dumpster.*

What are some of the best ways to destroy electronic documents?

Use data wiping software, as it permanently removes information by writing new, meaningless information on top of old information. CDs and DVDs can be shredded. Computer hard drives can be "magnetically degaussed," which uses extremely strong magnets to remove the magnetic encoding that stores data — which is a very affordable way to responsibly destroy old hard drives.

Refer to Chapter 4 of "Data Security — *Made Simpler*" for more information about these methods and potential resources to help.

What are some common myths about destroying data that I should be aware of?

Here are three examples:

1. *Breaking or smashing an old computer DOES NOT necessarily destroy the information it houses.* Just because you break the machine does not mean you're breaking the media where the data is stored (on the hard drive).
2. *Microwaving CDs and DVDs DOES NOT destroy the information on them, and can release toxic fumes into your microwave or cause a fire.*
3. *Placing data into the "Recycle Bin" on your desktop DOES NOT destroy the information.* Neither does clicking "Delete." It still exists and can be recovered.

Refer to Chapter 1 of "Data Security — *Made Simpler*" for more information.

What are the key things I should tell my customers in my Data Security Policy?

Here are some ideas to get started:

1. *If you are encrypting sensitive information in every site it is stored* — both stationary and portable — tell them that
2. *If you restrict access to sensitive data,* outline the key ways you're doing this (i.e., locking cabinets and closets, limited access to solely employees that need the information to do their job, etc.) — tell them that, too;
3. *Consider obtaining a third-party seal* that verifies your small business uses an appropriate level of security to protect your web site or your internet transactions.

Refer to Chapter 1 of "Data Security — *Made Simpler*" for other ideas of specific data security precautions you may be taking that are appropriate to communicate to your customers. But whatever you say you are doing, make sure you're doing it! And if you change the way you secure data, make sure you update your policy and your customer communications to reflect that change.

You can also refer to Chapter 5 of "Data Security — *Made Simpler*" for potential resources of companies that validate safety of web sites or provide online data security seals of approval.

Is there anything I should not communicate in my Data Security Policy?

Yes.

1. *DO NOT SHARE detailed information about your security systems that criminals might use that to evade them.*
2. *DO NOT tell customers there is no risk of ID theft, or that their information is "100% safe." No matter how hard you try to protect customer information, there is always a chance that someone may obtain it and misuse it.*
3. *DO NOT guarantee or promise that a customers' information can never be lost or stolen unless you tell customers what you will do if that promise if broken.*

Refer to Chapter 5 of "Data Security — *Made Simpler*" for more detailed

KELLEY DRYE BRYAN CAVE Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association

What type of "red flags" might signal suspicious behavior and an attempt at fraud?

Here are just a few examples:

1. *A "customer" opens a new account that contains suspicious elements... such as a P.O. Box for a home address or an email address that seems to have someone else's name.*
2. *A customer presents you with suspicious documents, such as an ID card that appears altered, different addresses on different forms of ID, or a P.O. Box as a home address.*
3. *Your (or one of your employees) notice unusual activity relating to a customer's account.*

What are the five (5) things small businesses should do to secure their online banking credentials (e,g, PINs, passwords, tokens, et)?

1. initiate payments under dual control. Ensure that all payments are initiated from your bank accounts only after the authorization of two employees.
2. update virus protection and security software. Ensure that all anti-spyware, anti-malware, and security software and mechanisms for all computer workstations and laptops that are used for online banking and payments are robust, up-to-date, and that there is a process for periodically checking that they remain up-to-date,
3. have dedicated workstations. If possible, restrict the use of certain workstations and laptops to be utilized solely for online banking and payments.
4. reconcile accounts daily. Monitor and reconcile accounts daily against expected credits and withdrawals. If unexpected activity is seen on your account, notify your financial institution immediately.
5. use robust authentication methods. Set up methods to access your accounts via multi-channel authentication.

Prepared for BBB by Dana Rosenfeld – Kelley Drye & Warren LLP and David Zetoony – Bryan Cave LLP
Content contributions from NACHA – The Electronic Payments Association