New Data Security Resources for Small Merchants

18 April 2018

Sylvia Auyeung

Diana Greenhaw

VISA

Disclaimer

Forward-Looking Statements

The materials, presentations and discussions during this meeting contain forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. These statements can be identified by the terms “will,” new,” "continue," "could," “accelerate,” and other similar references to the future. Examples of such forward-looking statements may include, but are not limited to, statements we make about our plans and goals regarding authentication, risk and fraud, the effect of developments in regulatory environment, and other developments in electronic payments.

By their nature, forward-looking statements: (i) speak only as of the date they are made, (ii) are neither statements of historical fact nor guarantees of future performance and (iii) are subject to risks, uncertainties, assumptions and changes in circumstances that are difficult to predict or quantify. Therefore, actual results could differ materially and adversely from those forward-looking statements because of a variety of factors, including the following:

- the impact of regulation, including its effect on issuer and retailer practices and product categories, and the adoption of similar and related laws and regulations elsewhere;
- developments in current or future disputes
- macroeconomic and industry factors such as: global economic, political, health and other conditions; competitive pressure on customer pricing and in the payments industry generally; material changes in our customers' performance compared to our estimates; and disintermediation from the payments value stream through government actions or bilateral agreements;
- systemic developments, such as: disruption of our transaction processing systems or the inability to process transactions efficiently; account data breaches involving card data stored by us or third parties; increased fraudulent and other illegal activity involving our cards; failure to maintain interoperability between our and Visa Europe's authorization and clearing and settlement systems; loss of organizational effectiveness or key employees; and
- the other factors discussed under the heading "Risk Factors" herein and in our most recent Annual Report on Form 10-K and our most recent Quarterly Reports on Form 10-Q.

You should not place undue reliance on such statements. Unless required to do so by law, we do not intend to update or revise any forward-looking statement, because of new information or future developments or otherwise.

Disclaimer

Notice

The information, recommendations or “best practices” contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations, programs or “best practices” may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance.

Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

Agenda

- Payment Security Landscape
- New Data Security Resources for Small Merchants
- PCI SSC Qualified Integrators and Resellers Program Updates
- Q&A Session

Payment Security Landscape

Data Security Landscape

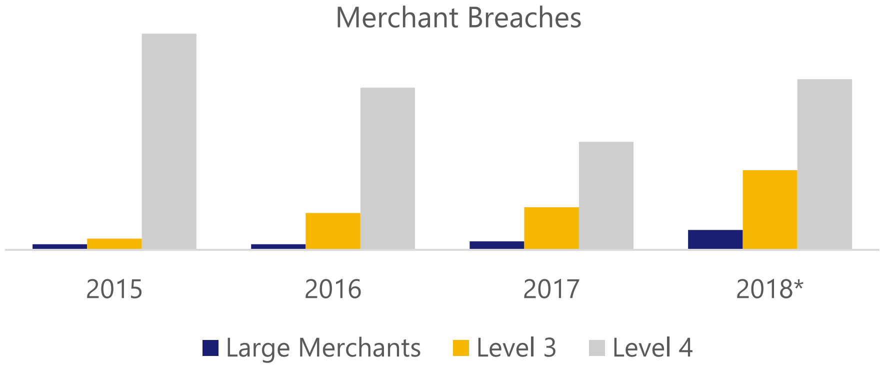
Breach Trends

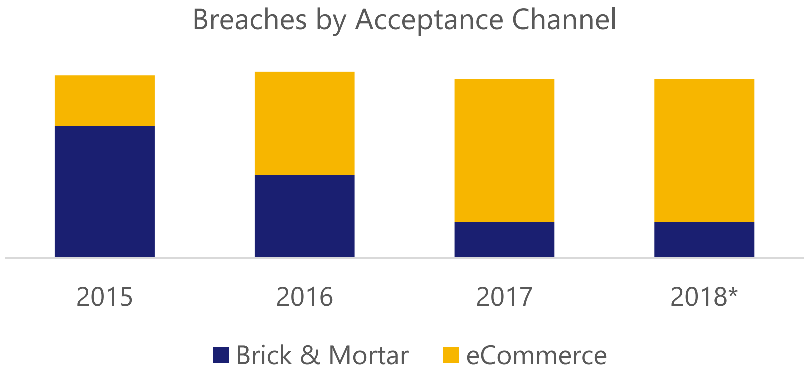
Breach Types

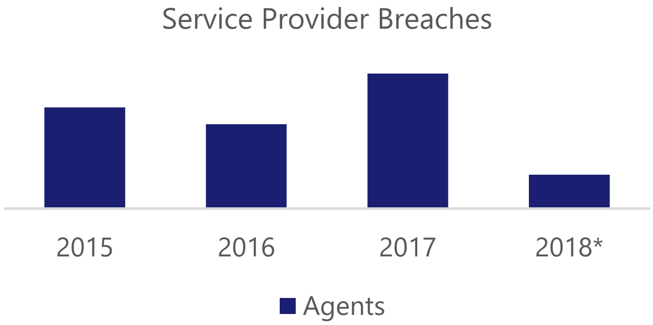
- Small merchants targeted more frequently than other organizations
- Number and impact of e-commerce compromises is increasing

Moving Beyond Merchants

- Criminals increasingly targeting service providers and data aggregators
- Financial institutions targeted for access to cash vehicles (ATM Attacks)


Merchant Breaches


Breaches by Acceptance Channel


Service Provider Breaches

*1 January 2018 – 31 March 2018

What Does This Mean for Small Merchants?

👎

- Small merchants continue to be a primary target for criminals
- Common errors and missing security controls remain the leading cause of breaches
- Non-compliant service providers can place small merchants at higher risk of compromise

👍

- Majority of small merchant breaches may be prevented with a few simple essential data security controls
- Visa maintains and publishes the Global Registry of Service providers to include registered, PCI DSS-validated agents
- PCI SSC recently published a new series of data security infographics and videos targeted to small merchants

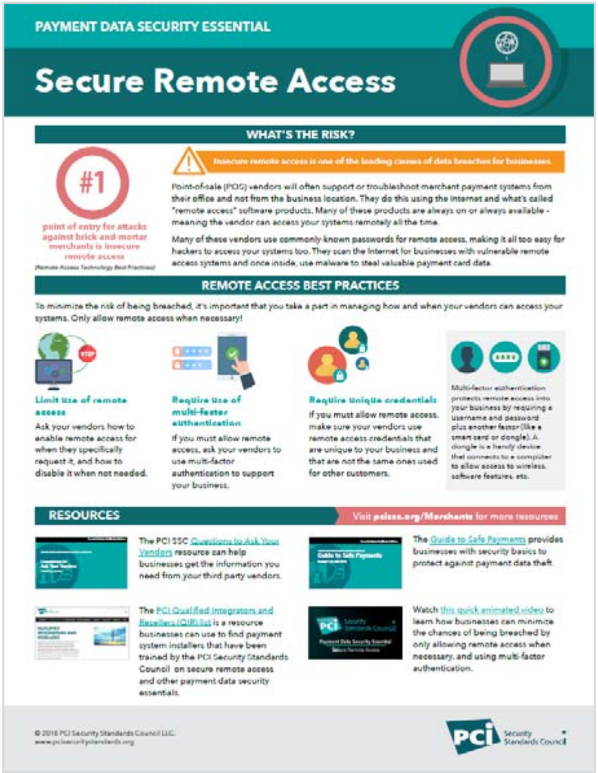
New Data Security Resources for Small Merchants

New Data Security Resources for Small Merchants

PCI SSC Infographics

Tips for Managing Top Vulnerabilities

Insecure Remote Access



PAYMENT DATA SECURITY ESSENTIAL

Secure Remote Access

WHAT'S THE RISK?

#1 point of entry for attacks against brick and mortar merchants is insecure remote access (Remote Access Technology Best Practices)

Insecure remote access is one of the leading causes of data breaches for businesses.

Point-of-sale (POS) vendors will often support or troubleshoot merchant payment systems from their office and not from the business location. They do this using the Internet and what's called "remote access" software products. Many of these products are always on or always available - meaning the vendor can access your systems remotely all the time.

Many of these vendors use commonly-known passwords for remote access, making it all too easy for hackers to access your systems too. They scan the Internet for businesses with vulnerable remote access systems and once inside, use malware to steal valuable payment card data.

REMOTE ACCESS BEST PRACTICES

To minimize the risk of being breached, it's important that you take a part in managing how and when your vendors can access your systems. Only allow remote access when necessary!

Limit use of remote access
Ask your vendors how to enable remote access for when they specifically request it, and how to disable it when not needed.

Require use of multi-factor authentication
If you must allow remote access, ask your vendors to use multi-factor authentication to support your business.

Require unique credentials
If you must allow remote access, make sure your vendors use remote access credentials that are unique to your business and that are not the same ones used for other customers.

Multi-factor authentication protects remote access into your business by requiring a username and password plus another factor (like a smart card or dongle). A dongle is a handy device that connects to a computer to allow access to wireless, software features, etc.

RESOURCES — Visit **pcisse.org/Merchants** for more resources

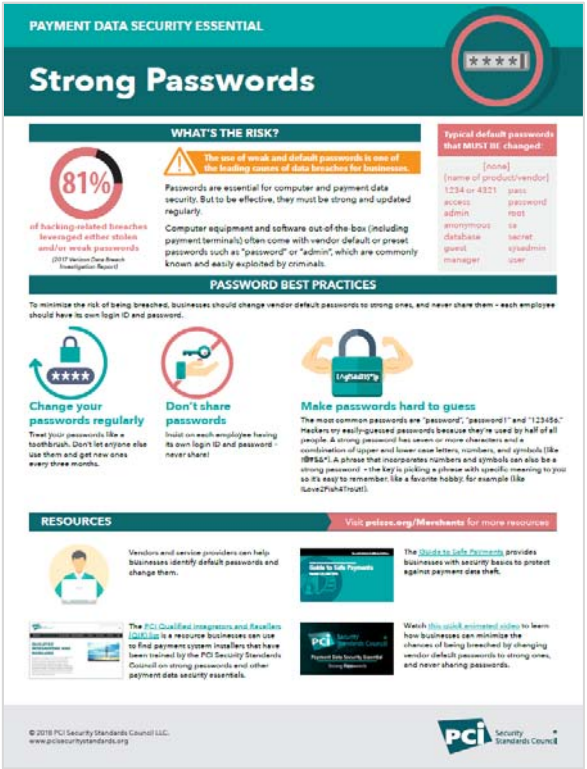
The PCI SSC Questions to Ask Your Vendors resource can help businesses get the information you need from your third party vendors.

The Guide to Safe Payments provides businesses with security basics to protect against payment data theft.

The PCI Qualified Integrators and Resellers (QIR) list is a resource businesses can use to find payment system installers that have been trained by the PCI Security Standards Council on secure remote access and other payment data security essentials.

Watch this quick animated video to learn how businesses can minimize the chances of being breached by only allowing remote access when necessary, and using multi-factor authentication.

Weak Passwords



PAYMENT DATA SECURITY ESSENTIAL

Strong Passwords

WHAT'S THE RISK?

81% of hacking-related breaches leveraged either stolen and/or weak passwords (2017 Verizon Data Breach Investigation Report)

The use of weak and default passwords is one of the leading causes of data breaches for businesses.

Passwords are essential for computer and payment data security. But to be effective, they must be strong and updated regularly.

Computer equipment and software out-of-the-box (including payment terminals) often come with vendor default or preset passwords such as "password" or "admin", which are commonly known and easily exploited by criminals.

Typical default passwords that MUST BE changed:

[none]
[name of product/vendor]
1234 or 4321
access
admin
anonymous
database
guest
manager
pass
password
root
sa
secret
sysadmin
user

PASSWORD BEST PRACTICES

To minimize the risk of being breached, businesses should change vendor default passwords to strong ones, and never share them – each employee should have its own login ID and password.

Change your passwords regularly
Treat your passwords like a toothbrush. Don't let anyone else use them and get new ones every three months.

Don't share passwords
Insist on each employee having its own login ID and password - never share!

Make passwords hard to guess
The most common passwords are "password", "password1" and "123456." Hackers try easily-guessed passwords because they're used by half of all people. A strong password has seven or more characters and a combination of upper and lower case letters, numbers, and symbols (like !@#$&*). A phrase that incorporates numbers and symbols can also be a strong password – the key is picking a phrase with specific meaning to you so it's easy to remember, like a favorite hobby, for example (like ILove2Fish4Trout!).

RESOURCES — Visit **pcisse.org/Merchants** for more resources

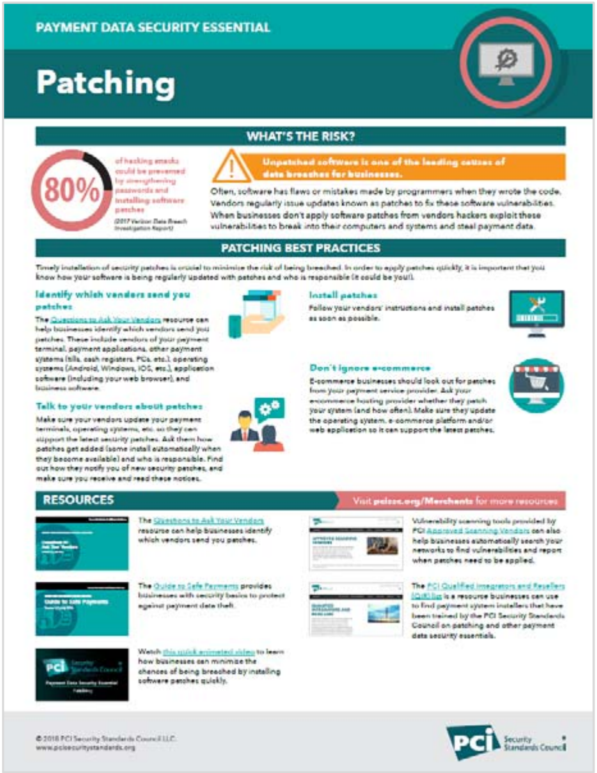
Vendors and service providers can help businesses identify default passwords and change them.

The Guide to Safe Payments provides businesses with security basics to protect against payment data theft.

The PCI Qualified Integrators and Resellers (QIR) list is a resource businesses can use to find payment system installers that have been trained by the PCI Security Standards Council on strong passwords and other payment data security essentials.

Watch this quick animated video to learn how businesses can minimize the chances of being breached by changing vendor default passwords to strong ones, and never sharing passwords.

Outdated Software



PAYMENT DATA SECURITY ESSENTIAL

Patching

WHAT'S THE RISK?

80% of hacking attacks could be prevented by strengthening passwords and installing software patches (2017 Verizon Data Breach Investigation Report)

Unpatched software is one of the leading causes of data breaches for businesses.

Often, software has flaws or mistakes made by programmers when they wrote the code. Vendors regularly issue updates known as patches to fix these software vulnerabilities. When businesses don't apply software patches from vendors hackers exploit these vulnerabilities to break into their computers and systems and steal payment data.

PATCHING BEST PRACTICES

Timely installation of security patches is crucial to minimize the risk of being breached. In order to apply patches quickly, it is important that you know how your software is being regularly updated with patches and who is responsible (it could be you!).

Identify which vendors send you patches
The Questions to Ask Your Vendors resource can help businesses identify which vendors send you patches. These include vendors of your payment terminal, payment applications, other payment systems (tills, cash registers, PCs, etc.), operating systems (Android, Windows, IOS, etc.), application software (including your web browser), and business software.

Talk to your vendors about patches
Make sure your vendors update your payment terminals, operating systems, etc. so they can support the latest security patches. Ask them how patches get added (some install automatically when they become available) and who is responsible. Find out how they notify you of new security patches, and make sure you receive and read these notices.

Install patches
Follow your vendors' instructions and install patches as soon as possible.

Don't ignore e-commerce
E-commerce businesses should look out for patches from your payment service provider. Ask your ecommerce hosting provider whether they patch your system (and how often). Make sure they update the operating system, e-commerce platform and/or web application so it can support the latest patches.

RESOURCES — Visit **pcisse.org/Merchants** for more resources

The Questions to Ask Your Vendors resource can help businesses identify which vendors send you patches.

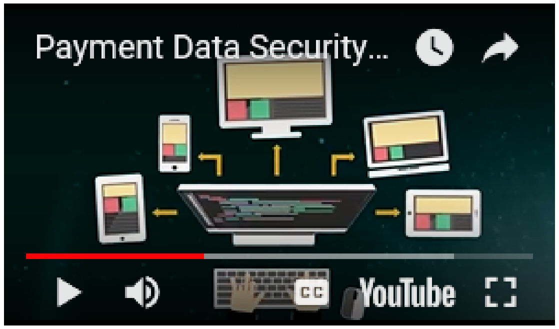
Vulnerability scanning tools provided by PCI Approved Scanning Vendors can also help businesses automatically search your networks to find vulnerabilities and report when patches need to be applied.

The Guide to Safe Payments provides businesses with security basics to protect against payment data theft.

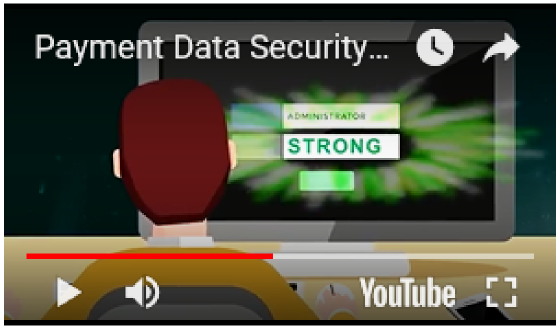
The PCI Qualified Integrators and Resellers (QIR) list is a resource businesses can use to find payment system installers that have been trained by the PCI Security Standards Council on patching and other payment data security essentials.

Watch this quick animated video to learn how businesses can minimize the chances of being breached by installing software patches quickly.

PCI SSC Data Security Essentials Video Series



Payment Data Security Essential: Secure Remote Access



Payment Data Security Essential: Strong Passwords

Payment Data Security Essential: Patching

All Videos Available Directly on the PCI Security Standards Council's YouTube Page

PCI Security Standards Council®

www.youtube.com/user/PCICouncil

VISA

PCI SSC Qualified Integrator and Reseller Program Update

Qualified Integrators and Resellers Program Update

- The PCI QIR program provides guidelines, training and qualification on security controls related to the installation of merchant payment systems
- PCI SSC is introducing program revisions to focus on the leading causes of small merchant breaches
- Changes also designed to increase the value of certification and expand opportunity for user participation

STREAMLINED CERTIFICATION for integrators and resellers:

- Reduced Cost
- Shorter Course Time
- Individual Certification

FOCUSED TRAINING on the 3 leading causes of payment data breaches:

- Weak Password Practices
- Insecure Remote Access
- Unpatched and Outdated Software

MERCHANTS BENEFIT by:

- Increased Pool of Integrators and Resellers Trained in Critical Security Controls

QIR Program Changes Result in **NO** Impact to Visa's Small Merchant Security Compliance Requirements

Visa Data Security Resources

Visa Data Security Resources

Visa Online Merchant Tool Kit provides helpful information to make a seamless EMV transition

- Streamline your chip migration www.VisaChip.com/businesstoolkit

Visa Data Security Website www.visa.com/cisp

- Alerts, Bulletins
- Best Practices, White Papers
- Past Webinars

Visa Global Registry of Service Providers www.visa.com/onthelist

- List of registered, PCI DSS validated third party agents

PCI Resources for Small Merchants https://www.pcisecuritystandards.org/merchants/

- Guide to Safe Payments, Common Payment Systems, Questions to Ask your Vendors
- Payment Data Security Essential: Video and Infographics

PCI Security Standards Council Website www.pcissc.org

- Data Security Standards, Qualified Assessor Listings, Data Security Education Materials

Q&A