New Data Security Resources for Small Merchants

18 April 2018

Sylvia Auyeung
Diana Greenhaw
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.
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)
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

Weak Passwords

Outdated Software

**Secure Remote Access**

**What's the Risk?**

As small and midsize businesses increasingly rely on remote access to their network, they're more vulnerable to attacks through weak controls or misconfigured systems. To prevent unauthorized access, you'll need to follow these best practices:

- **Limit use of remote access.** Ask your vendors to use remote access only when absolutely necessary and only for tasks that require it.
- **Require use of strong authentication.** If your vendors need to access your network, ask them to use strong authentication tools like multi-factor authentication. Make sure to check their credentials before allowing access.
- **Require strong passwords.** Use strong passwords that are unique to the vendor and that are not the same as those used by your own network.

**Tips for Managing Remote Access**

- **Implement strong authentication.** Use multi-factor authentication (MFA) to add an extra layer of security. MFA requires users to provide two or more pieces of evidence to sign in to a device or account.
- **Enforce strict password policies.** Require strong passwords that are at least 12 characters long and include a mix of letters, numbers, and symbols. Passwords should not be reused within a certain time period.

**Resources**

- Visit visa.com/members for more resources.

**Strong Passwords**

**What's the Risk?**

Weak passwords are a leading cause of data breaches. To prevent unauthorized access, you'll need to follow these best practices:

- **Employ proper password management practices.** Use strong, unique passwords for each online account. Consider using a password manager to help you create and remember strong passwords.
- **Use a combination of letters, numbers, and symbols.** Strong passwords should be at least 12 characters long and include a mix of letters, numbers, and symbols.
- **Avoid sharing passwords.** Never share your passwords with others, even if they ask you to do so. Passwords should be kept confidential, even from other members of your team.

**Tips for Managing Passwords**

- **Use a password manager.** Consider using a password manager to help you create and remember strong passwords. Password managers can also help you keep track of which passwords you use for which websites.
- **Change passwords regularly.** Change your passwords every few months or whenever you suspect that your password may have been compromised.

**Resources**

- Visit visa.com/members for more resources.

**Patching**

**What's the Risk?**

Outdated software is one of the leading causes of data breaches. To prevent unauthorized access, you'll need to follow these best practices:

- **Keep software up to date.** Regularly update all software to ensure that you have the latest security patches and fixes.
- **Patch known vulnerabilities.** Be sure to patch all known vulnerabilities as soon as they are released.

**Tips for Managing Patching**

- **Automate patching.** Consider using an automated patch management tool to help you keep your software up to date.
- **Test before deploying.** Before deploying any patches, test them in a controlled environment to ensure that they do not cause any issues.

**Resources**

- Visit visa.com/members for more resources.
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

www.youtube.com/user/PCICouncil
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 Online Merchant Tool Kit provides helpful information to make a seamless EMV transition
Visa Data Security Website [www.visa.com/cisp](http://www.visa.com/cisp)
  • Alerts, Bulletins
  • Best Practices, White Papers
  • Past Webinars
Visa Global Registry of Service Providers [www.visa.com/onthelist](http://www.visa.com/onthelist)
  • List of registered, PCI DSS validated third party agents
PCI Resources for Small Merchants [https://www.pcisecuritystandards.org/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](http://www.pcissc.org)
  • Data Security Standards, Qualified Assessor Listings, Data Security Education Materials