Machine Learning in the Payments Industry

24 May 2018

John Steensen

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

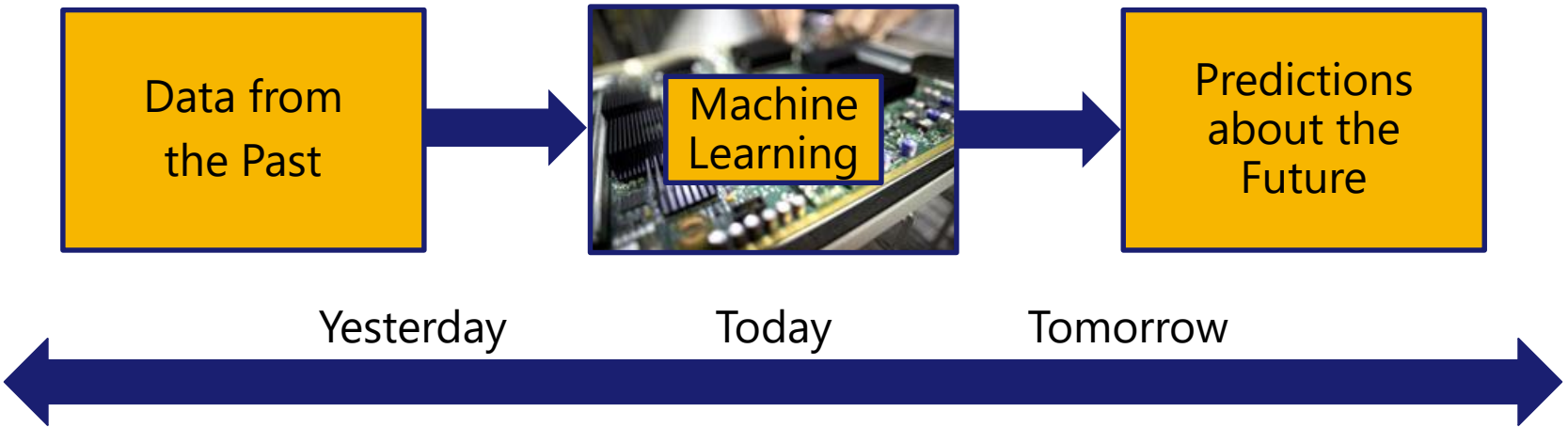
- A Brief Introduction to Machine Learning
- Machine Learning Applications in the Payment Industry
- Decision Making with Machine Learning
- Threats from Machine Learning-based Attacks
- Managing and Monitoring of Machine Learning
- Questions and Answers

A Brief Introduction to Machine Learning

VISA

What is Machine Learning?

- Machine Learning is a part of computer science that "gives computers the ability to learn without being explicitly programmed".
  Arthur Lee Samuel, 1959



What is Learning?

- Learning is the process of acquiring a body of knowledge, usually with the intent of performing some actions based upon that knowledge.

By identifying the most influential cause-and-effect relationships from the past, a machine can learn to make accurate predictions about the future.

Find Arsenic

Find Gold

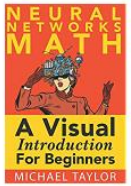
Machine Learning is Becoming Widely Used

"In recent years many successful machine learning applications have been developed, ranging from data-mining programs that learn to detect fraudulent credit card transactions, to information-filtering systems that learn users' reading preferences, to autonomous vehicles that learn to drive on public highways."[1]

Machine Learning: A Technical Approach To

Hands-On Machine Learning with Scikit-Learn

Neural Networks and Deep Learning: Deep Learning

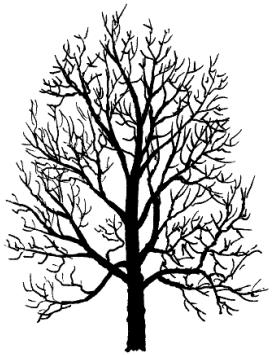


The Math of Neural Networks

[1]Machine Learning by Tom M. Mitchell, 1997 (p. xv)

Machine Learning Applications are Models

- Models are simplified approximations to the real world.



- Most models are built to support a specific activity within a specific environment.

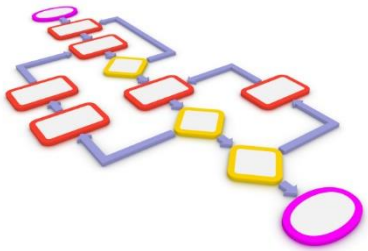
Models are Built upon Data

- In machine learning the data columns are referred to as “features”. Getting the data ready to use is called “feature engineering”.

- Although payment systems generate a lot of data, because of industry standards, much of it is well structured which reduces the effort needed to prepare it for use in machine learning algorithms.

Implementing Machine Learning

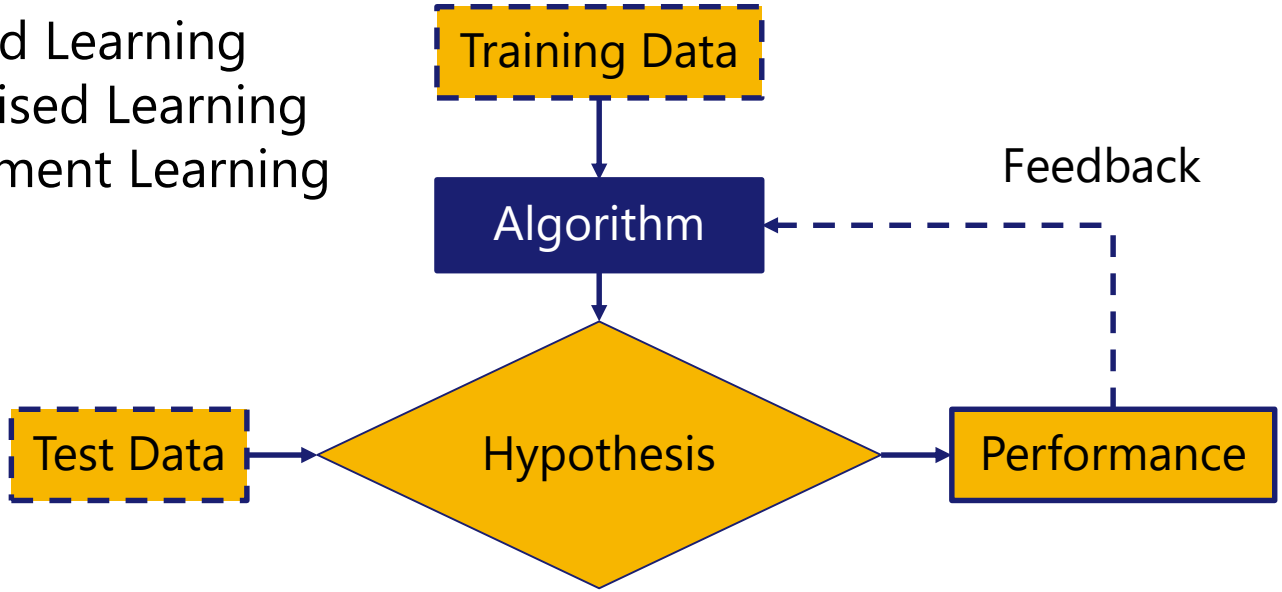
- Machine learning uses many different algorithms.
- Algorithms are just step-by-step processes to calculate a result.



- Data is needed by these algorithms to “train” them and to “test” them.
  - Some algorithms need data that is expertly prepared to exacting specifications before they can work.
  - Some algorithms can analyze large volumes of raw data (often called “Big Data”) and prepare the data themselves.

Types of Machine Learning Algorithms

- Supervised Learning
- Unsupervised Learning
- Reinforcement Learning



- Each of these have specific problem areas that they are best suited for.
- Part of the data scientist's job is to know which of these algorithm types to apply to the business situation they are facing.

Supervised Learning

- Step 1: Identify the outcome variable which is to be predicted
- Step 2: Identify the set of input variables called predictors
- Step 3: Generate a mathematical function that maps the input variables to outcome variable. This mapping process is called “training” and is repeated until the model achieves a desired level of accuracy on the training data and the testing data.
- This algorithm is called “Supervised” because there is outcome data that is already known to be correct and the training is supervised by the data scientist in trying to find an acceptable mapping function.

Unsupervised Learning

- Using this algorithm, there is not any specific target or outcome variable to predict or estimate.
- It is used for clustering a population into different groups. For example, it is widely used for segmenting customers into different groups for specific intervention or marketing activities.
- The algorithm is “tuned” by rerunning with different parameters until the desired granularity or group-size is achieved.
- These algorithms are called “Unsupervised” because they identify the clusters or groupings by themselves.

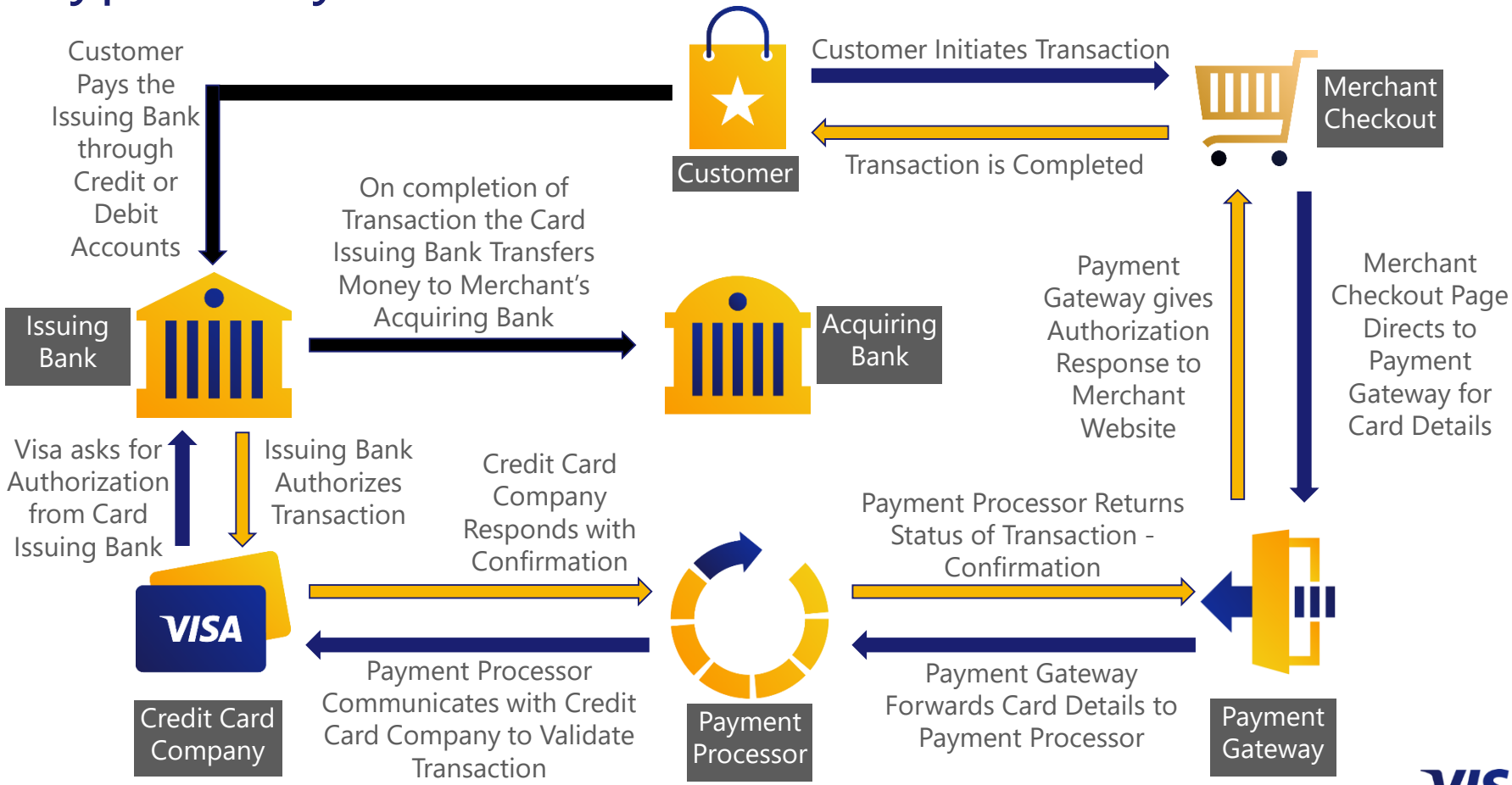
Reinforcement Learning

- Using this algorithm, the algorithm is trained to make specific decisions.
- The algorithm is exposed to an environment where it trains itself repetitively using trial and error.
- This algorithm learns from past experience and tries to capture the best possible knowledge to make accurate business decisions.
- It is call “Reinforcement” learning because the training reinforces the desired behavior from the algorithm.

Machine Learning Areas of Application in the Payment Industry

VISA

A Typical Payment Flow



Payment Flow Metrics Determination

- **WHO** → Is initiating the transaction?
  Was the recipient of the transaction?
- **WHEN** → Is the transaction initiated?
- **WHERE** → Is the transaction initiated from?
- **HOW** → Was the transaction initiated?
  Often were transactions initiated?
- **WHAT** → Was the transaction trying to accomplish?
  Is the value associated with the transaction?

What are Machine Learning's Unique Advantages?

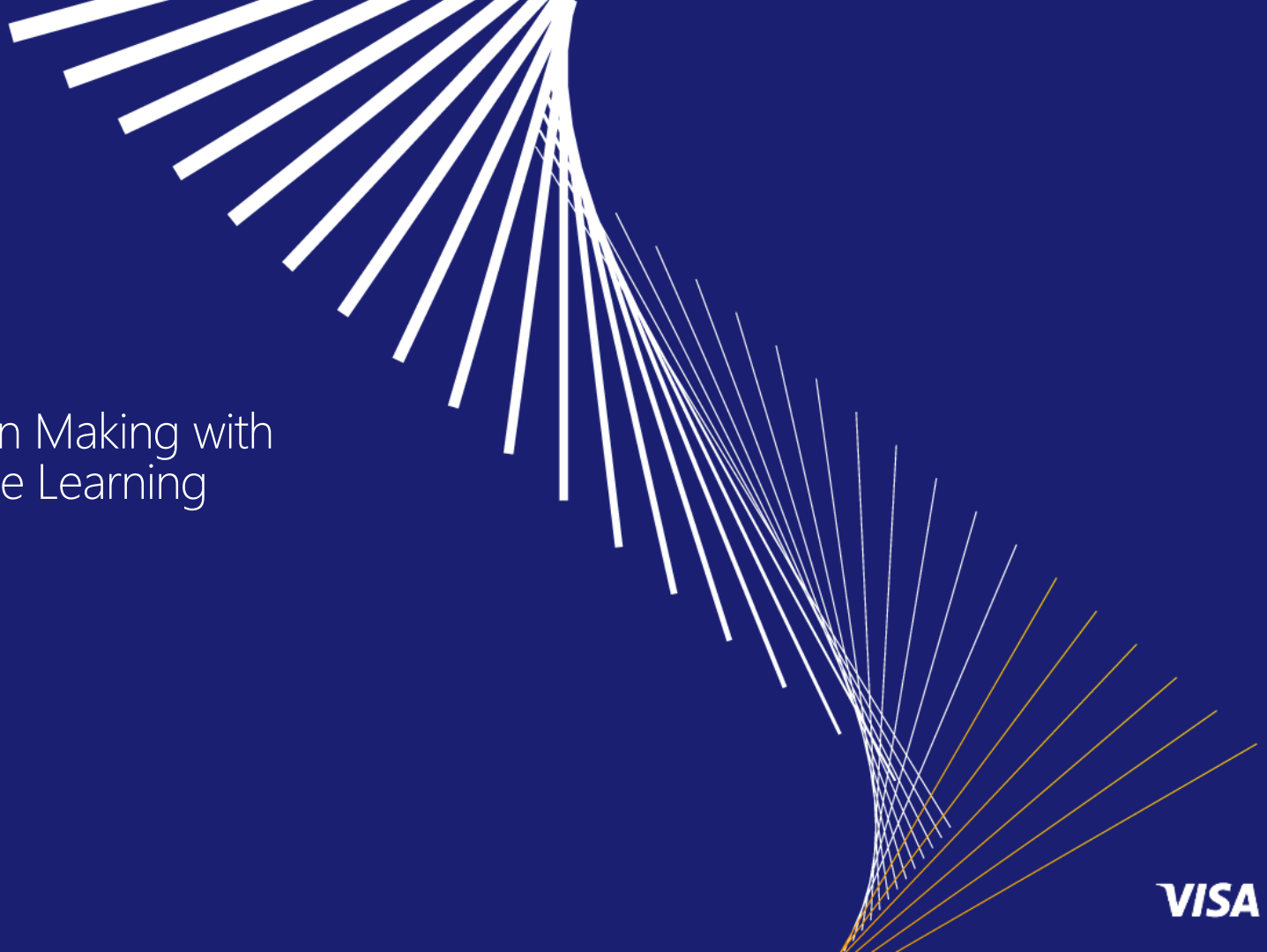
- Based upon real data, not human interpretations of data.
- Can incorporate massive amounts of data.
- Can typically outperform business rule-based processing approaches.
- Algorithms can be combined into something called "ensembles" allowing for more variety in the solutions.

Fighting Fraud

Machine learning fraud fighting strengths:

- Facilitating real-time decision-making power that allows for evaluation of huge numbers of transactions
- Improving accuracy of decisions resulting in detection of subtle or non-intuitive patterns to help identify fraud and avoid erroneous false positives

Decision Making with Machine Learning



VISA

Machine Learning “Accuracy” is a Business Decision

- Machine learning is about understanding the past to make predictions about the future ~ and some of those predictions will be wrong.
- Inaccurate rules logic may result in rejections of valid transactions or “false negatives” leading to revenue loss or customer dissatisfaction.
- Always remember that machine learning, like any tool or technology, is there to serve the needs of the business.

Tuning Your Machine Learning Algorithms

- Machine learning algorithms must be accurate:
  - Algorithms tied too tightly to past behavior are “over-training”.
  - Algorithms tied too loosely to past behavior are “under-training”.
- Determine the acceptable business balance between “false positives” (approving payments that should have been rejected) and “false negatives” (rejecting payments that should have been approved.)
- Algorithms can be re-trained on often as necessary to keep up with changing trends in the business environment.

Threats from Machine Learning-based Attacks

VISA

Machine Learning is a Tool for the Threat Actor

- Machine learning can allow threat actors to first gain a better foothold in the payment ecosystem to accomplish their mission.
- The threat actor may utilize machine learning to help in disguising a bad payment transaction as a good one.
- Remember that machine learning needs data to be properly trained so, to the extent you can, deny the availability of that data to the threat actor.

Threat Techniques Enhanced by Machine Learning

- Cloaking or “Wolf among the Sheep”

- “Outrun the Cops”

- “Wait out the Cops”

- “Friendly Microbe”

Managing and Monitoring of Machine Learning

VISA

Managing Machine Learning

- Machine learning applications are models that are simplified approximations to the real world.
- If the nature of the specific activity, or the environment within which that activity takes place changes, you will need assurance that the model is still relevant.
- If your operating environment is dependent upon machine learning then you need to assess, or reassess on a regular basis, the premises and data underlying the machine learning application you are using. This is a new area of change management.

Monitoring Machine Learning

- How do you know that a machine learning application is becoming outdated?
- Monitor for a change in effectiveness of the machine learning application. For example, are you getting more of a specific result than you expect?
- If possible test the machine learning application outside of the rest of the system and review the metrics you first used to evaluate the application.

Summary

Opportunities for Action

- Machine learning has an important role to play in supporting a robust and safe payment environment.
  - Acquire trained professionals or develop staff through training and certification.
  - Train Internal Audit on risks associated with machine learning.
- Threat actors will try and use this technology to their advantage.
  - Deny criminals the ability to access data to train models.
- Proper monitoring and managing of this technology is essential.
  - Obtain feedback on the use of machine learning.
- Model Risk Management (MRM) programs should include all critical models.
  - Determine applicability of MRM to machine learning-based models.

Question & Answer

Visa Data Security Resources

Visa Data Security Resources

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