PREPARING FOR THE UNEXPECTED:

EMERGENCY CARD REPLACEMENT & MASS ISSUANCE STRATEGIES

By Ray Wizbowski,
Vice President of Marketing,
Financial Vertical
Datacard Group

DatacardGroup

BREACHES AND OTHER EMERGENCIES

STRATEGIES FOR REPLACING CARDS & RESTORING TRUST

The well-documented financial card breaches of late 2013 and early 2014 shine a bright light on two key concerns for banks, bureaus and other large card issuers.

The first concern, of course, is prevention. After dissecting recent high-profile breaches, security experts generally conclude that more than 90% of the breaches that have occurred in recent years were preventable given the right strategies (which, interestingly, are focused more on policy and process than technology. Clearly, the deployment of EMV cards and other multi-factor solutions will provide extra lines of defense against financial cybercrime. However, few if any security experts are claiming that breaches can be stopped all together. The vulnerabilities surrounding personal data and financial credentials are simply too numerous and too varied to get to 100% prevention. Also, cyber criminals tend to be smart and adaptive, which means issuers will need to do their best to remain one step ahead.

The second concern centers on the replacement of both cards and trust across a national — or global — cardholder base. Getting high-quality cards into the hands of customers enhances spending power and minimizes the disruption in revenues for financial institutions. It also helps strengthen the issuers' brands and positions them as responsive and customer-centric.

TOP CAUSES OF DATA SECURITY BREACHES

Verizon published a study in early 2014 that analyzed the root causes for more than 600 breaches that occurred in 2012. The report identified these primary causes of data security breaches.

Weak or Stolen Credentials. Valid credentials are used in almost every serious breach. Credentials not protected with two-factor authentication techniques are especially vulnerable.

Unsuspecting Employees. Senior executives are often the targets for spearfishing attacks, which simply require users to open the wrong PDF or PowerPoint document.

Phishing. Nearly a quarter of all attacks involve phishing. If hackers send anywhere from 3-10 phishing emails to a user, they are almost guaranteed to gain access.

Hacking. Cyber thieves often use SQL injections to gain access to websites and their underlying servers.

TOP CAUSES OF DATA SECURITY BREACHES (Continued)

Malware. Installation of malware by hackers after they gain access to a system accounts for more than 70% percent of all breaches

Spyware. Spyware enables hackers to steal credit card data from point-of-sale transactions and account credentials entered by users into online bank accounts

Too Few Internal Barriers. Most data takes just hours or even minutes to steal. Forensic experts recommend focusing on creating barriers that lengthen the time required for hackers to explore and locate relevant systems

Too Many Permissions. The most costly breaches studied involved data stored "at rest" in databases and file servers. Memory scraping malware, spyware and skimmers were responsible for a majority of the other stolen data

Stored or Unencrypted Payment Information. The most vulnerable, critical and desired data is payment information and account credentials. These and other data should be encrypted and never stored.

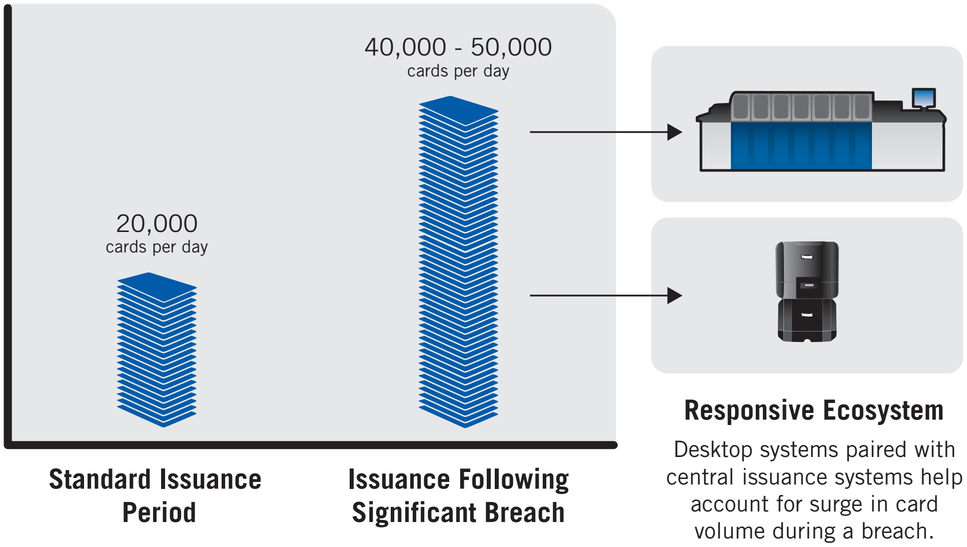
Shell Services. Attackers with access to corporate networks use shell services — such as SSH and RPC — to move laterally through an organization.

ADDRESSING CONSUMER DEMAND WITH RESPONSIVE CARD OPERATIONS

In the days following a significant breach in late 2013, it was extremely important for banks and credit unions to work with millions of affected consumers. Many brands were at stake. When consumer perception is hindered, it can be detrimental to an organization's brand and overall customer confidence. Given the timing of the latest breach — just before Christmas — customers wanted their cards replaced very quickly. But such a large data breach and the need for large-scale card reissuance can cause a significant backlog for card issuers, prolonging emergency card replacement and creating an even greater challenge for consumer confidence.

For financial institutions, there was further cause for concern as they saw their daily card issuance volumes more than double. Not only did financial issuers need to complete their regular run-rate of reissues, they now had to deal with mass issuance of many replacement cards for those at risk. For example, many operations were optimized for approximately 20,000 cards per day, but after the breach, there was a jump to 40,000-50,000 new cards per day for some issuers — presenting a difficult challenge for many operations.

There is a way to address this, however, by ensuring card operations are prepared and have the necessary strategies in place to increase service levels and optimize operations. There is a growing trend for financial institutions to provide instantly issued, fully personalized cards at the bank branch. During this last crisis, financial institutions that had already deployed this solution were able to reach out to their customers and offer to replace their card right in the branch location. As a result, cardholders were able to receive permanent magnetic stripe credit and debit cards within minutes and could start using their card right away at point-of-sale terminals. As it turned out, instant issuance was an optimal complement to these financial institutions' central card operations –providing a much-needed outlet for the unexpected card volumes. While systems and staff in central locations had to scramble to make quick adjustments, tens of thousands of cards were issued on-demand in branch locations.



Responsive Ecosystem

Desktop systems paired with central issuance systems help account for surge in card volume during a breach.

In addition to alleviating volume issues, many of the banks and credit unions offering instant issuance leveraged the breach to promote this benefit to their customers who were otherwise unaware of the offering. The message delivered to consumers was that these financial institutions were prepared, cared about their customers, were taking measures to protect cardholders and offered a means to resolve the issue quickly.

Utilizing both central and instant issuance models for mass issuance of replacement cards ultimately helped financial organizations provide unprecedented customer service, increased security and tremendous cost savings. In a world where almost everything is instant, the banking industry needs to respond with relevant technology to ensure consumers have the best possible banking experience. When there is a need for a replacement card, the financial institutions that are best prepared to meet their customers' needs have consistently reported higher customer retention rates and incremental revenue gain from the instantly issued cards.

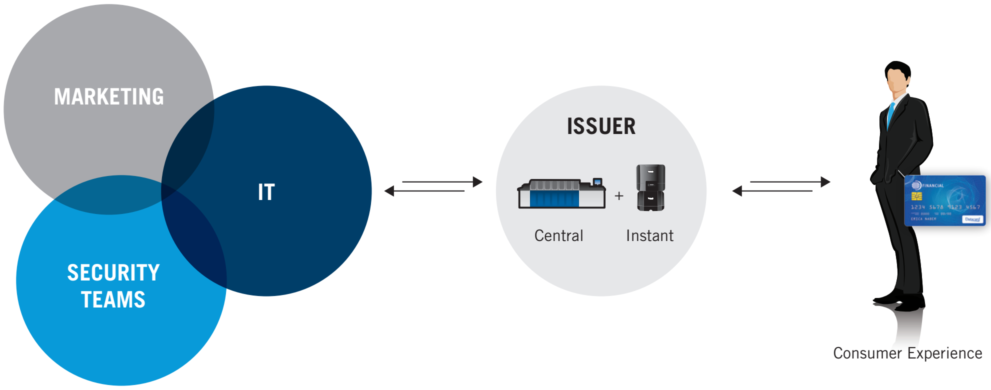
CONSTRUCTING AN EFFECTIVE ISSUANCE ECOSYSTEM

Financial organizations' vision continues to evolve "the ultimate consumer experience." Implementing instant issuance as a complement to the central card operations ecosystem clearly does this — not only from an emergency card replacement standpoint, but also as a means to pave the way for various future technology advancements in the payments industry. For example, in addition to on-demand issuance of traditional magnetic stripe credit and debit cards, instant issuance infrastructures can be configured to issue mobile wallets, mobile commerce applications and EMV smart cards.

The question then becomes "how do we get started to better prepare for the next breach?" We've outlined some key considerations to help you establish a timeline.

EVALUATE CURRENT CARD OPERATIONS

An optimized central and instant issuance ecosystem requires cross-functional cooperation from marketing (consumer experience), operations, IT and security teams within the issuance institution. Ideally, the ecosystem enables the vision the marketing team has for the emerging consumer experience. This means consumer-driven criteria must serve as the foundation for the expanded ecosystem. Since a majority of the day-to-day responsibility of managing, optimizing and advancing the issuance ecosystem rests with the operations team, their insights are required to ensure the ecosystem that is designed can actually be built — and sustained. Data security and compliance responsibilities reside with IT and security teams. While they make decisions about technologies, deployment and technical support, they also must address the policies and processes required for operating instant issuance systems in branch locations.



CONSTRUCTING A FUNCTIONAL ISSUANCE ECOSYSTEM

CONSIDER TECHNOLOGIES NEEDED FOR INSTANT ISSUANCE

There are various technologies that can easily complement centralized card operations. Think about the holistic instant issuance solution — including the software and hardware needed to implement in branch locations. Software can be implemented directly at the branch level or through a hosted model, and can help with reporting capabilities. In addition, there are various desktop printers that can be implemented at branch locations that offer several personalization and printing capabilities. For example, there are unembossed or embossed personalization technologies; various printing resolutions and options for background images; magnetic stripe or smart card encoding capabilities, among others.

By understanding what type of instant issuance technologies are on the market, it will better equip issuers to implement an instant issuance solution that can fit and grow with their needs, and be an extension of their central issuance operations. This ultimately protects their investments and sets them up to future-proof their solutions so that they can easily add in capabilities such as mobile or EMV.

FACTOR IN DATA SECURITY

While adding instant capabilities to an issuance ecosystem adds new “endpoints,” the data security requirements are mostly policy- and process-oriented. The same technologies and processes used for protecting cardholder data and financial credentials in a central issuance environment are simply extended to the broader instant issuance network. Ideally, all data — in use, in transit and at rest — is always encrypted and never stored on a server, issuance device or anywhere else on a network. Protecting the new instant issuance endpoints requires multi-factor credentials for employees accessing the system and compliant procedures for managing passwords and other credentials.

It is also important to consider the underlying security architecture that must be in place to protect every transaction, every connection and to ultimately protect every end user and device’s identity when consumers or bank employees are accessing the network. It is critical that this security be completely hidden to the end user. Just as we see today, there is limited tolerance for excessive security requirements such as entering security codes from hard tokens, completing detailed Q&As or even navigating username password schemes.

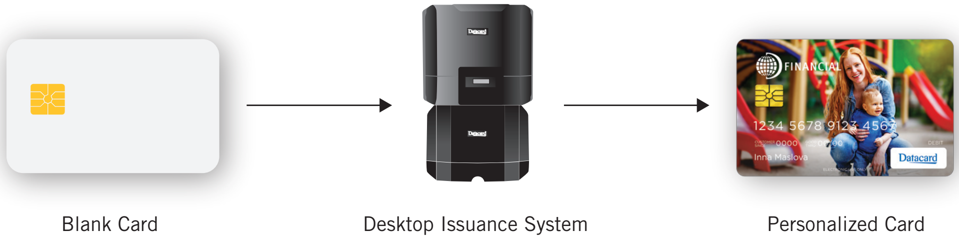
Making the security architecture as seamless as possible while never compromising the integrity of cardholder data — from all users’ perspectives — is the ultimate goal. There are real time fraud detection technologies on the market today that transparently monitor cardholder behavior over time, identify anomalies, and automatically calculate risk associated with particular transactions and/or cardholder behavior. If risks are identified, the software should be able to increase authentication requirements and only complete transactions if identification criteria are met.

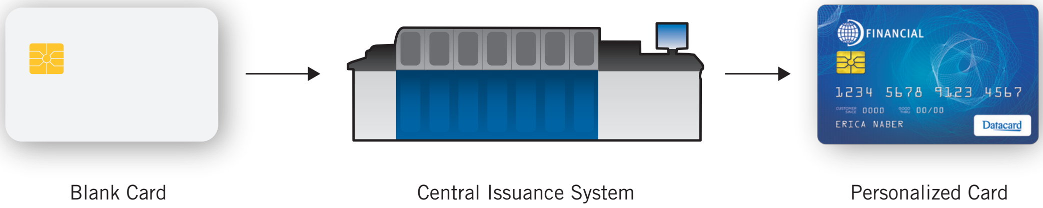
THE ROLE OF INCREASED CARD VAULT EFFICIENCIES

Card stock is another area to think about when preparing for mass issuance of emergency card replacements. While personalizing and delivering replacement cards after a breach can be a challenge, that process cannot take place if the right cardstock is not available in the right place and at the right time. Often times this can be overlooked, but it is a key consideration for card issuers when thinking about how to be prepared for a breach in the future.

If a breach happens, not having the proper card stock readily available in the card vault can be a potential bottleneck when issuers need to move fast. It's known that vault management costs have plagued issuers since financial cards were introduced. Millions of dollars are wasted every year on producing and storing cardstock that is not needed because of overruns or card designs being retired. The data breach threat accentuates this problem. If card volumes double overnight, the vault cost problem escalates at approximately the same rate.

Think about how you can alleviate this potential bottleneck by having on-demand printing technology that allows issuers to keep more generic cardstock in their vaults, then use on-demand printing technology to create specific card types. Essentially — blank card stock in, a customized card out. Today, this is highly important as consumers are demanding more personalized offerings and more customization — which means more small jobs and more "on-the-fly" personalization for operations teams. Adding the urgency of mass emergency card replacement to the docket creates complex management issues. Having the capability to personalize blank card stock – both centrally or instantly — helps with costs, efficiency, flexibility and continues to provide personalized services to consumers, which adds to the overall "consumer experience" element of differentiation.





CARD DELIVERY & THE CONSUMER EXPERIENCE

Data breaches clearly create a need to communicate with customers. Issuers want to explain how they are protecting consumer data, what they are doing to ensure product continuity and how customers can get answers to their questions. From a central issuance perspective, much of this highly targeted, one-to-one communication can be accomplished with new card delivery systems. Customized card carriers — in various sizes and in full color — can be printed as part of the inline issuance process. The same data that drives card personalization drives the custom form printing process. Advanced card delivery systems, which can be configured inline or standalone, can also be used to deliver promotional messages or required information, such as terms and conditions.

THINK BIG
DELIVER BIG
THE CONSUMER JOURNEY
ACTIVATION INSTRUCTIONS
THINK BIG DELIVER BIG
FINANCIAL
1234 5678 9123 4567
CUSTOMER SINCE 0000
GOOD THRU 00/00
MICHAEL SHIN
Datacard
DatacardGroup

CONCLUSION — CRISIS RESOLUTION & THE CONSUMER EXPERIENCE

The next several years in the financial market could broadly be called the “age of the consumer experience.” Banks that leverage technology to anticipate and align with consumer demands will have a great advantage in the battle for customer loyalty. How banks and other issuers react to crises, such as a data breach, will directly contribute to the composite picture of the consumer experience. The technologies and strategies deployed to gain market share and loyalty advantages are the same as the ones required to deal with data breaches and other crises. Exploring concepts such as central and instant issuance infrastructures gives banks and other consumer marketers the agility and flexibility to quickly address crises — or capitalize instantly on new marketing opportunities.

DatacardGroup

CORPORATE HEADQUARTERS
11111 Bren Road West
Minnetonka, Minnesota 55343-9015
Phone: +1 952 933 1223
www.datacard.com
info@datacard.com