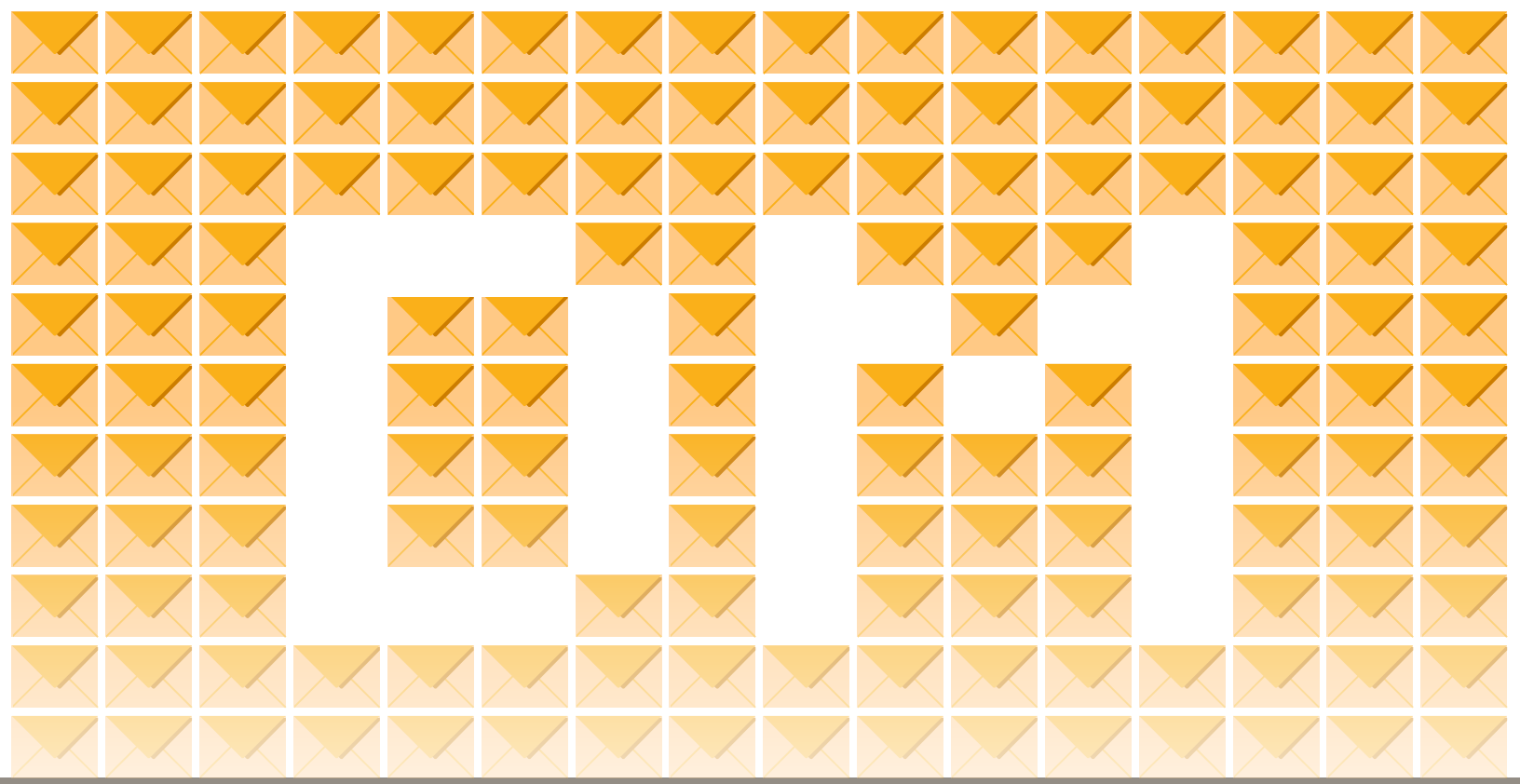

2013

DMARC

HOW JP MORGAN ADOPTED DMARC TO STOP PHISHING ATTACKS AND PROTECT THEIR CUSTOMERS

Agari 100 S. ELLSWORTH AVENUE, SUITE 400 : SAN MATEO, CA 94401 : 650.627.7667

WHEN JP MORGAN CHASE DECIDED TO ADOPT DMARC TO STOP PHISHING ATTACKS AND PROTECT ITS BRAND, THE PROBLEM WAS MUCH BIGGER THAN IT ANTICIPATED

"DMARC is a Triple Play. It gives banks a way to reduce their operating costs, deliver a better customer experience, and protect their brand."

– Jim Routh, Global Head of Application and Mobile Security, JP Morgan Chase

"We estimated that our customers as a whole received maybe a million phished emails from cybercriminals abusing our brand," explained Jim Routh, Managing Director and Global Head of Application, Internet and Mobile Security at JP Morgan Chase.

Once JP Morgan Chase deployed DMARC with Agari, they learned the number was closer to a billion.

"We were stunned," he continued. "Over a billion emails per year, purporting to come from our domain that are not ours, and many of them are phishing emails with malicious intent. Phishing emails are extremely damaging to our brand," Routh explained.

"Like any large bank, we rely on email for marketing and for servicing our customers, and we send out about 4 billion emails a year for these purposes."

JP Morgan Chase realized that its brand was eroding through the email channel because customers -- and potential customers -- were unable to determine whether an email from the bank was legitimate, Routh said.

JP Morgan Chase realized that its brand was eroding through the email channel because customers -- and potential customers -- were unable to determine whether an email from the bank was legitimate, Routh said.

"For any financial service organization that sends email, and most of us do that quite a bit, we are actually competing with fraudulent email senders for customer mindshare," Routh explained.

"And their tactics, which have become much more sophisticated, are causing a disastrous customer experience and serious brand damage," he continued. "So we're spending more money on email and getting less return because we're competing with fraudulent email."

JP Morgan Chase evaluated its options and embraced the DMARC (Domain-based Messaging Authentication and Controls) standard to stop phishing attacks, restore its brand and protect its customers.

Routh continued, "We were impressed with the collaboration between Google, eBay and the vision of industry leaders such as Patrick Peterson, CEO and Founder of Agari."

"You should be able to secure the online channels that you use to communicate with people"

"The concept is simple. You should be able to secure the online channels that you use to communicate with people," explained Patrick Peterson, describing the decision to form the DMARC standard. "When you receive email that is protected by Agari," Peterson explained, "you can trust that the email you're getting is really from whom it claims to be from; criminals should not be able to step into your space and defraud your consumers."

INCREASED THREAT OF PHISHING

"Measure DMARC by measuring the decrease in call volume that's related to brand erosion from email. You can attribute the decrease to the improvement in the email ecosystem over time."

– Jim Routh, Global Head of Application and Mobile Security, JP Morgan Chase

Yet, as JP Morgan Chase learned, cybercriminals are doing just that, defrauding consumers on a massive scale. In fact, a study by RSA published in 2012 documented a 19% increase in phishing attacks with approximately 32,500 attacks launched each month.

Peterson explained, "Cybercriminals have invested in a massive infrastructure that can send billions of spam and phish emails per day. Historically, there's been nothing whatsoever that brand owners can do about that."

Not surprisingly, as the volume of phishing attacks has increased, so have the monetary losses. RSA statistics show that global losses grew 32% year-over-year to over $1.4 billion. That suggests that each of last year's 390,000 phishing attacks inflicted $3,580 in costs per incident.

"Unfortunately, most companies learn about phishing attacks when the phone starts to ring," explained Peterson. Security, JP Morgan Chase

But where do these costs come from? And when does a company learn that their customers are the target of a phishing attack? "Unfortunately, most companies learn about phishing attacks when the phone starts to ring," explained Peterson. "By then, the horse has left the barn and the damage has already been done."

During one phishing attack, Nacha.org – the electronic payments association which administers the ACH Network – described the toll on its customer support operations. Keith Burmaster, Director of Systems Technology, recalled the impact on their operations. "On a normal day, we usually get 1,500 customer issues per day. During the peak of this attack, we were receiving 9 million issues per hour."

While some argue that any publicity is good publicity, when it comes to protecting customers from cybercriminals, companies that have been subjected to a phishing attack are also bombarded by harsh publicity. "Today, customers don't stay silent," explained Peterson. "If they've been a victim of a phishing attack, odds are, they will tell their

"Today, customers don't stay silent," explained Peterson. "If they've been a victim of a phishing attack, odds are, they will tell their friends on Facebook and Twitter."

friends on Facebook and Twitter."

Indeed, a recent American Express survey confirmed that Americans tell an average of 9 people about good experiences, and almost 16 (nearly two times more) about poor experiences. Moreover, Touch Agency confirmed that roughly 80% customer service tweets are negative or critical in nature.

"It's time for every financial institution to step up to the plate and drive adoption of DMARC for their email ecosystems, and to put our industry on the map as a leading industry in information security risk management compared to every other industry."

– Jim Routh, Global Head of Application and Mobile Security, JP Morgan Chase

As the groundswell of publicity increases, public opinion sharpens and increasingly, courts are ruling in favor of customers, repeatedly claiming that companies have a fiduciary responsibility to protect customers from phishing attacks.

In fact, in the Experi-metal phishing attack (which caused the custom auto-parts manufacturer to lose over $500K) Michigan courts argued that the company's bank Comerica failed to protect its consumers from phishing attacks. "A bank dealing fairly with its customers under these circumstances would have detected and stopped the fraudulent wire activity earlier," explained Judge Patrick Duggan of the U.S. District Court for Eastern Michigan in his ruling.

A study by Frost and Sullivan determined that 71% of information security officers listed "protecting their brands," as a key focus of their jobs, yet phishing attacks continue to erode brand trust.

"Customers are 42 percent less likely to do business with you if you are being targeted by a phishing attack"

"Customers are 42 percent less likely to do business with you if you are being targeted by a phishing attack," added Peterson, "regardless of whether or not your customers are actually getting tricked into giving up their information."

JP Morgan didn't want to take a chance; it adopted DMARC by partnering with Agari to put a stop to phishing attacks. "We're making the organization more efficient; we're reducing risk to our customers; and we're getting a lift in terms of where we're spending money today on email marketing campaigns," Routh continued. "Holistically, I think the business case is pretty compelling."

"We've got a partner in Agari," Routh added. "We're going to continue to promote and support those vendors across the email ecosystem that are DMARC-compliant. We'll identify them on our website and encourage broader adoption within the financial services community."

At first, Routh said, the bank implemented an authentication capability for all email sent to customers, ultimately notifying ISPs that only authenticated email originating from the bank's domain would be allowed. All other fraudulent, illegitimate email would be blocked from being delivered to the end customer. However, a number of third-party systems legitimately sending out email on the bank's behalf was caught in the web cast by the policy.

"Essentially it became more of a vendor management issue in terms of the email service providers that are sending email on our behalf, but it was a little more complex than that," he said. "We also found campaign management tools that were implemented either by a third party, or even other divisions, that were sending out emails. So the sources of email generation within a large enterprise are numerous."

Agari allowed the bank to identify each sender and establish standard practices and procedures in its third-party governance process. Any new third party coming on board that was going to send email would know that it had to authenticate properly or have a subdomain designated.

"The other challenge is in domain registration, so that any new domains that are registered are automatically authenticated and adopt the appropriate standards like DMARC for the authentication. That became an exercise to adjust our practices and do education awareness," Routh said.

Finally, JP Morgan Chase established a program to communicate the new policy to all marketing professionals involved with generating, designing and implementing email campaigns.

The Agari intelligence "is what gave us the capability to understand the scope of this, but it involved a lot of different functions within the bank to bring that together and to be able to pull this off," he said.

"Elimination of that fraudulent email not only improves the customer experience and reduces risk to our customers, it creates a lift in terms of the response rate for our existing email campaigns that we're carefully crafting and spending quite a bit of money on. There's a value proposition to getting a revenue generation opportunity simply through the implementation of a program with a risk-management objective," he said.

> ***"Elimination of that fraudulent email not only improves the customer experience and reduces risk to our customers, it creates a lift in terms of the response rate for our existing email campaigns that we're carefully crafting and spending quite a bit of money on."***

Routh added, "we've used Agari and implemented DMARC successfully for a little over a year from start to where we are at this point in time and we're quite pleased both with the results of the program and with the services that Agari has provided.

In the next month we expect to have over 90 percent of the fraudulent email blocked, so we're very pleased with the progress and the results."

Agari