

Brief Title



- As phishing increases banks will need to do more on reverse authentication
- User education will be required for some types of technology

KEY MESSAGES

Online banking has grown, as has the range of things that customers are doing online

The number of people going online for at least part of their banking services is on the increase across the globe, thanks in part to the growth of broadband connectivity, and in part to greater familiarity and comfort with the internet banking concept. For this same reason, people are doing more in their online banks than just consulting their balances: a growing number of them are also transferring funds.

Banks are increasing IT spend on online services and online security this year

Datamonitor research shows that banks are increasing their IT spending on their online channel generally this year, improving usability but also increasing the security around access to their internet services.

There are opportunities in client-side and back-end authentication technologies

There are opportunities for technology vendors in both the products banks are putting in their customers' hands for 2FA/MFA and at the back end, in systems that can provide greater levels of information in real time about someone who is trying to log on to a website, informing the bank as to how likely it is that they are who they say they are. While the US has deployed more back-end technology to date while Europe has gone more for the client side, Datamonitor believes there is room for each type of technology to expand its footprint in the other geography and for both to grow in Asia/Pacific.

The US has a broader definition of 2FA/MFA than Europe

Due to the earlier and widespread take-up of hardware token technology, there is a tendency in Europe to think of it as synonymous with 2FA/MFA. By contrast, due to the non-prescriptive way US regulators approached the subject, banks in that geography count other types of technology, including the back-end systems that increase information for the authentication decision, under the same heading.

Mobile phones are gaining traction as a channel for delivering a second factor

With the ever greater ubiquity of mobile phones, they are an obvious channel for delivering a second authentication factor, which sits well with the need for 2FA/MFA to use more than one channel to circumvent man-in-the-middle attacks.

A tiered approach to online security is advisable

Some of the technology covered in this report is expensive, particularly when it has a hardware component and will entail full-time helpdesks to support it. Therefore banks should think of different levels of online banking security for different categories of customer, varying from the person who stays at home and always banks from a home PC to an international traveler who may be using their BlackBerry in Beijing one day and the PC in their son's bedroom the next. Vendors would do well to embrace and recommend this concept rather than present their product as the silver bullet for all online security threats.

As phishing increases banks will need to do more on reverse authentication

With phishing exploits becoming ever more sophisticated and attacks increasingly adopting a multi-channel approach that combines the phone with the PC and more, banks must recognize the need, in their outbound communications with their customers, to prove to them that they are who they claim to be, in what is known as reverse authentication. Any B2C technology that can also be used in this way will be doubly valuable to a bank, and its vendors should highlight that fact.

User education will be required for some types of technology

Any security system is only as good as its users, since the best key in the world is useless if someone forgets to lock the door. As banks move to deploy more security on the client side, this will mean educating their customers on how to use the technology and what to do if it does not perform as they expect it to, which may indicate that they are being phished, for instance. Technology vendors, reseller partners and specialist consultancies should look to help banks with this requirement.

TABLE OF CONTENTS

Overview	1
<i>Catalyst</i>	1
<i>Summary</i>	1
Key Messages	3
<i>Online banking has grown, as has the range of things that customers are doing online</i>	3
<i>Banks are increasing IT spend on online services and online security this year</i>	3
<i>There are opportunities in client-side and back-end authentication technologies</i>	3
<i>The US has a broader definition of 2FA/MFA than Europe</i>	3
<i>Mobile phones are gaining traction as a channel for delivering a second factor</i>	3
<i>A tiered approach to online security is advisable</i>	3
<i>As phishing increases banks will need to do more on reverse authentication</i>	4
<i>User education will be required for some types of technology</i>	4
Market opportunity	8
<i>Online banking has grown, as has the range of things customers are doing online</i>	8
<i>Banks are increasing IT spend on online services and online security this year</i>	11
<i>There are opportunities in client-side and back-end authentication technologies</i>	16
Technology Evolution	17
<i>Adoption of 2FA/MFA has varied markedly by region</i>	17
<i>The US has a broader definition of 2FA/MFA than Europe</i>	19
<i>The FFIEC's non-prescriptive approach has spawned alternative technologies in the US</i>	20
<i>Mobile phones are gaining traction as a channel for delivering a second factor</i>	20
Customer Impact	21
<i>Online security must be integral to banks' business</i>	21
<i>A tiered approach to online security is advisable</i>	21
<i>As phishing increases banks will need to do more on reverse authentication</i>	22
<i>User education will be required for some types of technology</i>	22
Competitive Landscape	23
<i>Client-side technologies</i>	23
<i>Back-end technologies</i>	29
Go to Market	34
<i>Recommend a mixture of technologies</i>	34

Table of Contents

<i>Disruption to existing infrastructure is to be discouraged</i>	34
<i>Banks will need help with user education</i>	34
<i>Delivering technology as a service will appeal to smaller US and German institutions</i>	34
<i>Channel partners will be key in such accounts</i>	35
<i>Countries with greater banking concentration prefer to buy products</i>	35
<i>The fight against fraudsters will go on, so a long game may be in order</i>	35
APPENDIX	36
<i>Definitions</i>	36
<i>Methodology</i>	38
<i>Further reading</i>	39
<i>Ask the analyst</i>	39
<i>Datamonitor consulting</i>	39
<i>Disclaimer</i>	39

TABLE OF FIGURES

<i>Figure 1:</i>	<i>Percentage of US adults who “do some internet banking” (i.e. not necessarily daily)</i>	<i>10</i>
<i>Figure 2:</i>	<i>European banks’ investment priorities for payments in 2009</i>	<i>12</i>
<i>Figure 3:</i>	<i>North American banks’ investment priorities for payments in 2009</i>	<i>13</i>
<i>Figure 4:</i>	<i>European banks’ channel investment priorities for 2009</i>	<i>14</i>
<i>Figure 5:</i>	<i>North American bank’s channel investment priorities in 2009</i>	<i>15</i>

MARKET OPPORTUNITY

Online banking activity is on the increase, both in terms of the number of account holders doing it and the variety of activities being carried out, with a growing trend towards transactions that entail an actual transfer of funds.

This in turn encourages criminals to focus more closely on the online channel as a source of revenue and so increases the risk for banks and their customers. This scenario, together with regulatory requirements for additional security around online banking, results in a market opportunity for technology vendors in the area of products that can be distributed to account holders to provide an extra factor, as well as of technologies that can be deployed in the banks' networks or delivered as a service, to further inform the authorization decision.

While bank branches are still very much part of our urban landscape, the move towards online banking as a complement to visiting a branch, if not a wholesale replacement, seems inexorable. Research shows that, at least in developed world markets, more people are doing at least some banking online, and an increasing proportion of them are carrying out online transactions involving the transfer of funds.

However, the trend towards more internet banking is leading to criminals' increased focus on the opportunity that the online channel now represents. On the one hand, information security exploits have become more explicitly financial in their motivation over the last decade, with the script kid in his bedroom being replaced by the professional cybercriminal. Meanwhile, on the other, the opportunity to steal money without donning a mask and brandishing a revolver in a bank branch has increased exponentially.

Equally, the sophistication of exploits has increased, with criminals leveraging multiple vectors to achieve their nefarious ends. There are man-in-the-middle attacks (MITM), cross-site scripting and social engineering, as well as the standard viruses, Trojans, key loggers and screen scrapers. These all contribute to the collection of confidential data and/or the hijacking of the account holder's online banking session to change the amounts and destinations of fund transfers. General enterprise information security vendors have been talking about 'blended threats' (i.e. ones that use more than one vector to attain their goals) for a while, and the phrase is clearly pertinent in the context of exploits that compromise online banking security as well.

Online banking has grown, as has the range of things customers are doing online

Online banking services have been around for over a decade now, and have already undergone a considerable degree of evolution, from so-called PC banking, which involved having a software client on the customer's machine to establish a secure connection, to the browser-based activity that is now the norm. Datamonitor has even pondered where internet banking might go next, given the challenge/opportunity represented by the emergence of so-called Web 2.0 technologies such as blogs, wikis, mashups and, most recently, Twitter (see Datamonitor reports *Online Banking in the Age of Web 2.0*, DMTC2192 and *Web 2.0 in Online Banking: A Progress Report*, BFTC2311).

Statistics from a number of markets show that, as the technological underpinning of these services has evolved, so the number of people engaging in some form of online banking has increased and, just as importantly, the percentage using their online service to transfer funds is also growing year-on-year.

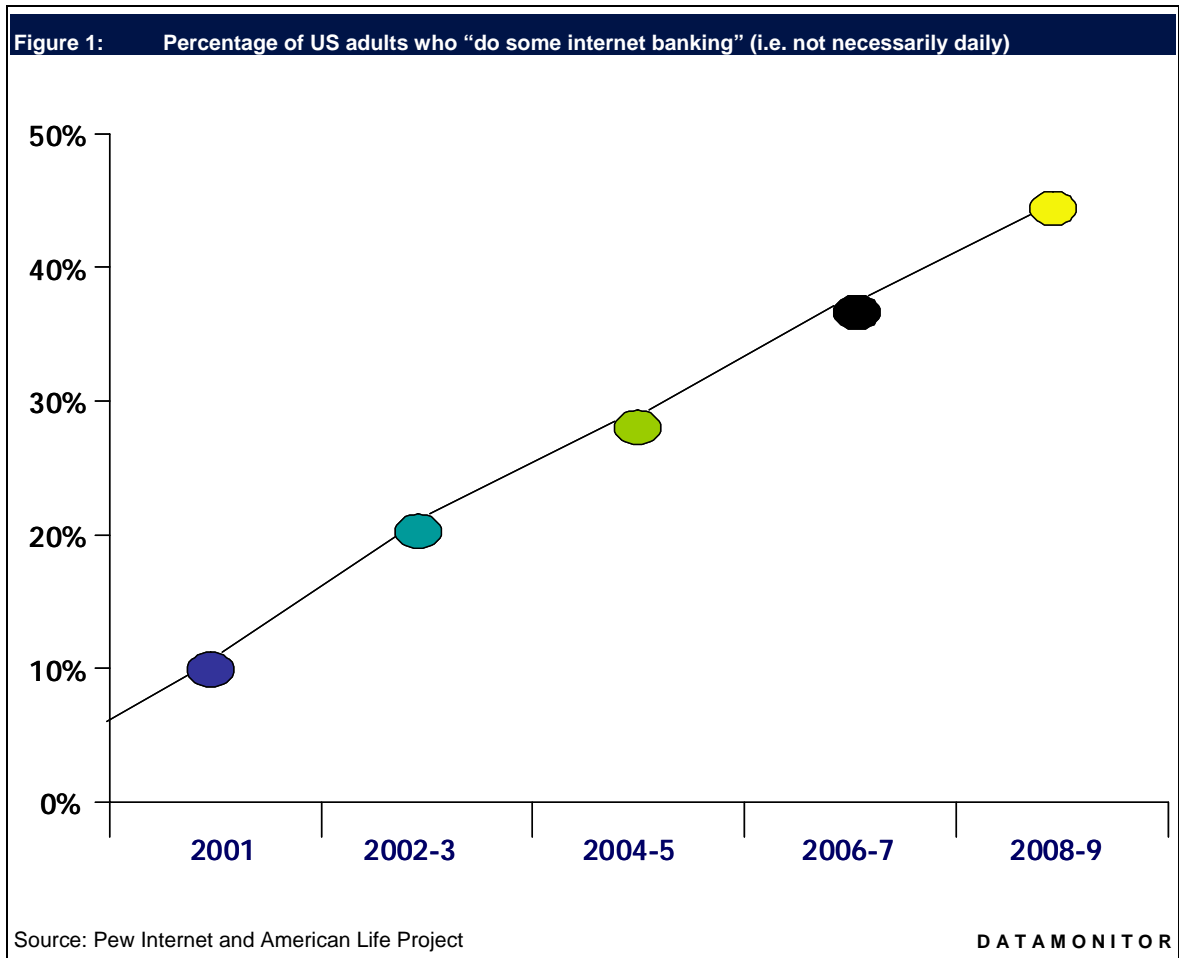
More account holders are banking online

Taking the UK as an example, statistics from the trade body, the UK Payments Administration, show that 21.5 million adults used the internet in 2008 to manage their main current account, the equivalent of more than half of all adults with regular access to the internet. Approximately 80% of users had been using the internet to access their main current account for more than 12 months, compared with 61% five years earlier.

The UK is by no means exceptional in this context. With broadband internet access approaching ubiquity in most developed world markets and online banking operations now a longstanding part of the service offering from all leading institutions, consumers are increasingly accepting the online channel as a way of managing their personal finances and their relationship with their bank.

While the US has no exact equivalent of the UK Payments Administration, there is the Pew Internet & American Life Project. This is one of seven projects that make up the Pew Research Center, which describes itself as “a nonpartisan, nonprofit ‘fact tank’ that provides information on the issues, attitudes and trends shaping America and the world.” The project produces reports exploring the impact of the internet on families, communities, work and home, daily life, education, health care, and civic and political life.

Among its statistics on online activities, 2000–09, Pew reveals that the percentage of US adults (both internet users and non-users) who replied positively to the question of whether they “Do any internet banking” rose from 10% in 2000–01 to some 42% in 2008–09 (see Figure 1), while the percentage who do some internet banking daily (again as a percentage of the entire adult population, including non-users of the internet) went from 4% to 18% over the same period.



More account holders are transferring funds online

Moreover, online banking increasingly entails more than just checking balances and verifying that cheques paid in have cleared. The UK Payments Administration's research also shows that, while the most popular actions in online current account banking last year were still checking account balances and statements, used by 96% and 82% of users, respectively, almost three-quarters of those banking online transferred money between accounts, and more than half used it to set up regular payment arrangements, pay bills or make other transfers or payments.

The move from PC to browser-based banking was a step up in terms of ease of use, and the prospect of Web 2.0 features being introduced will only intensify this trend. This, together with greater familiarity and increased confidence in banks' ability to carry out instructions received online, has contributed to this growth in the percentage of online banking that involves the transfer of funds.

The increasing popularity of online banking raises its profile for fraudsters

This scenario represents both an opportunity and a challenge to the banks themselves, as they can provide basic services to a growing percentage of customers online and thus tailor their more expensive branch operations to enhancing their

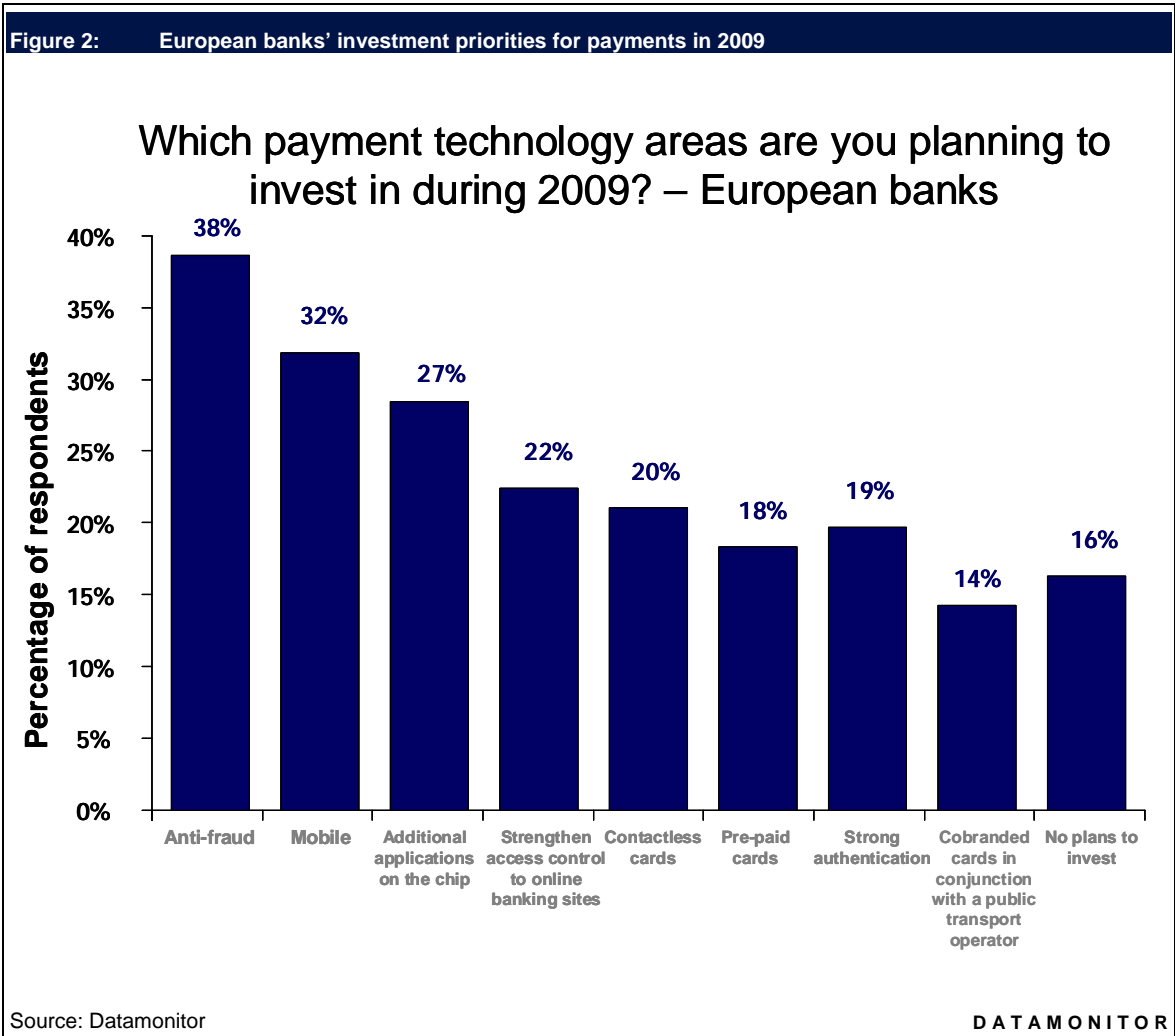
customer relationships (see Datamonitor, *Branch Strategies for the 21st Century in European Retail Banking*, DMTC2252). However, it also means that banks must step up the infrastructure that they have in place for securing their customers' online activity, for two reasons:

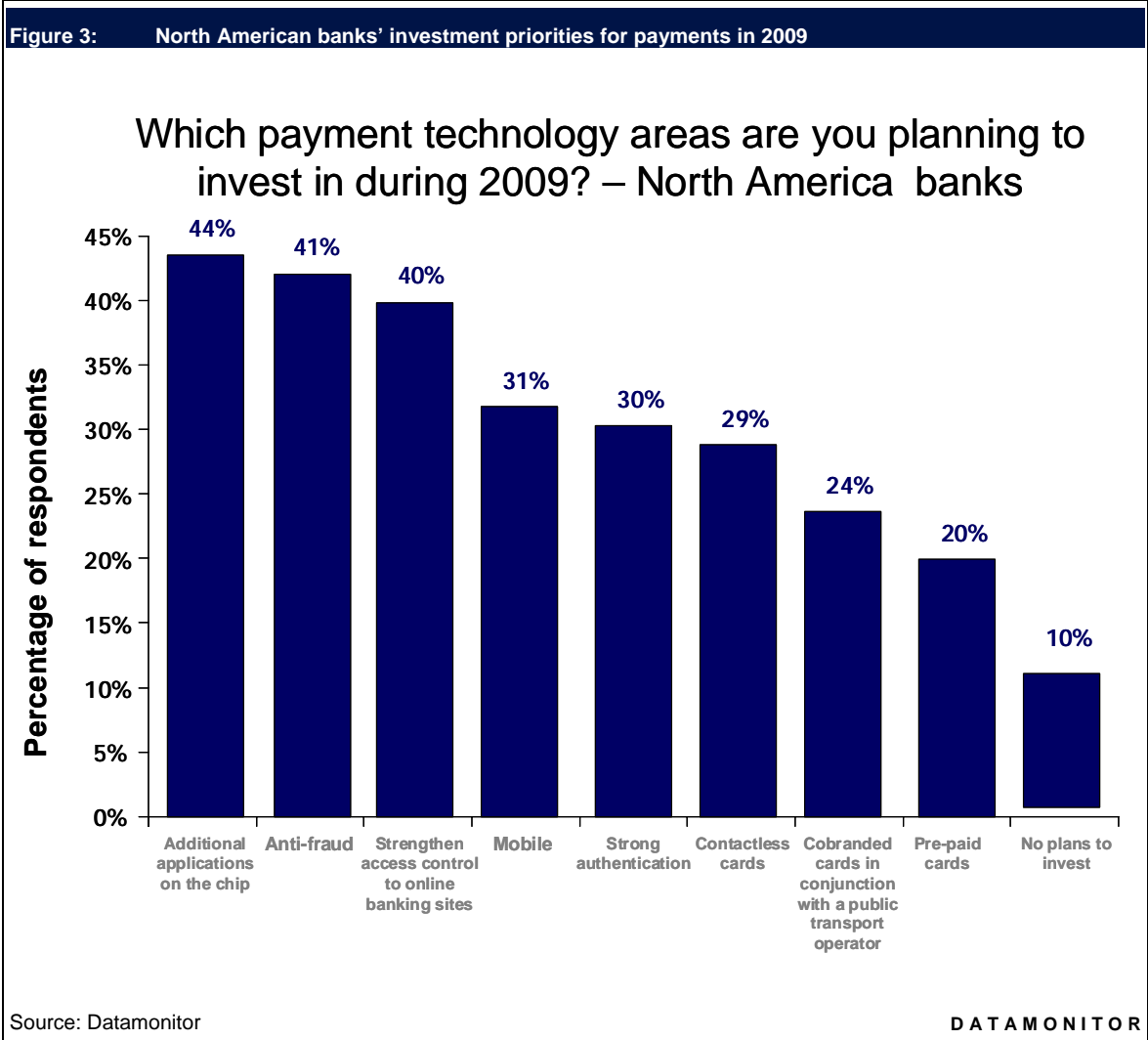
- More customers are going online and more of what they are doing online involves the actual transfer of funds.
- These developments attract the attention of fraudsters, for whom the online channel is becoming an increasingly lucrative source of potential revenue.

Banks are increasing IT spend on online services and online security this year

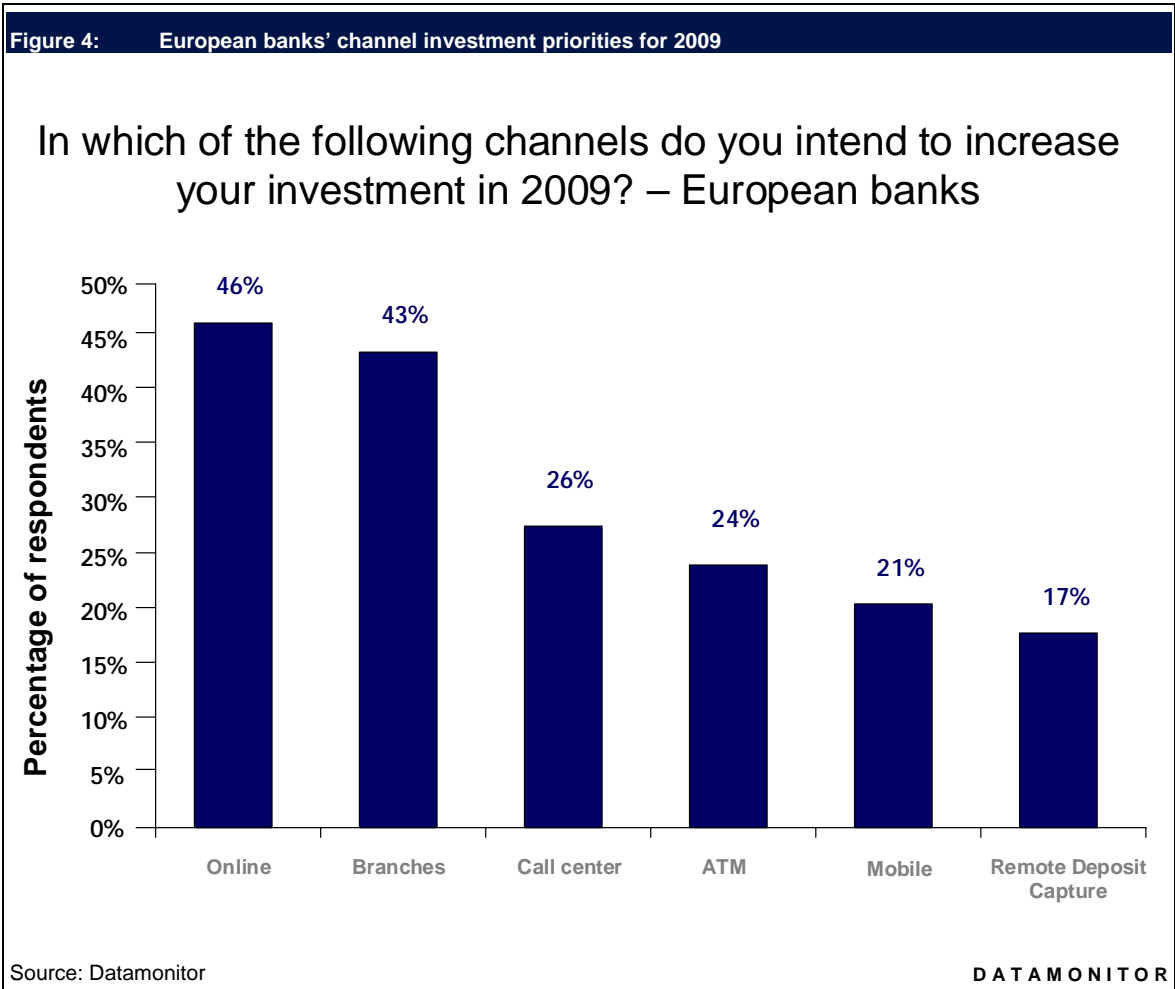
The fact that there is demand from banks for technology to enhance the security surrounding their online offerings is borne out by Datamonitor's primary research on IT spending in the sector. Datamonitor's most recent surveys (*Business Trends: North American Retail Banking Technology Spending Strategies 2009 (Customer Focus)*, DPTC0056, and *Business Trends: European Retail Banking Technology Spending Strategies 2009 (Customer Focus)*, DPTC0024) reveal banks' desire to step up the security infrastructure for internet banking.

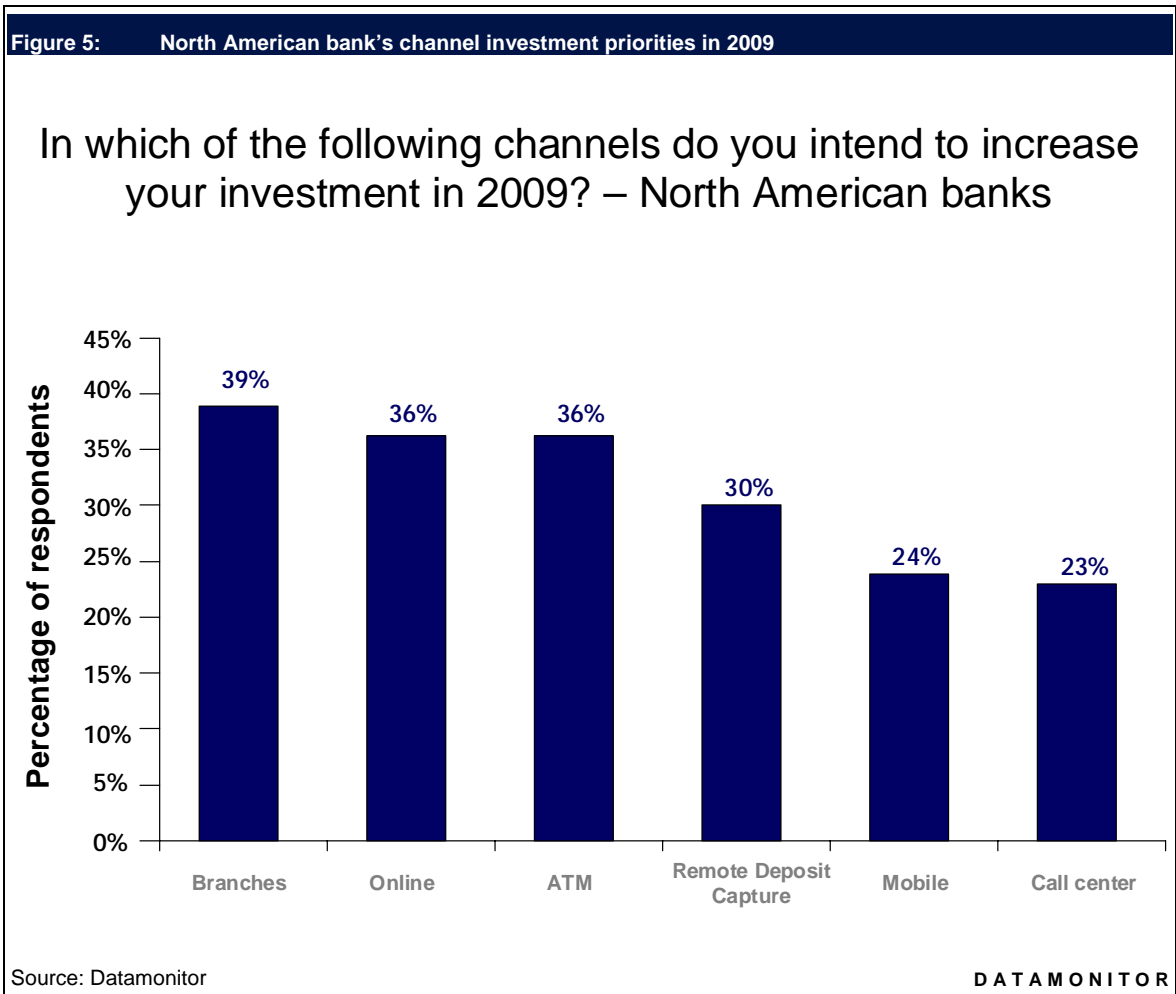
As shown in Figures 2 and 3, when asked "In which payment technology areas are you planning to invest during 2009?", the option "Strengthening access control to online banking sites" ranked third for banks in North America, having been selected by 40% of respondents. This option ranked fourth in Europe, having been chosen by 22% (the other option that came in higher in Europe was m-payments).





Meanwhile, Figures 4 and 5 show that, with regard to their IT spending priorities by channel (as against by payment type), online ranked highest for Europeans, with 46% of respondents singling it out for investment in 2009. Online came in joint second (behind branches) in North America, with 36% of respondents saying that they believe it is highly important to spend on that channel.





This situation represents a major opportunity for a range of vendors in segments within information security technology such as authentication and behavioral analysis, provided that they can craft their messaging to the banking industry so that it reassures potential customers that their products can be evolutionary and accretive to banks' existing infrastructure, rather than revolutionary and substitutive of what they currently have in place.

There are multiple reasons for this approach. Firstly, there is the inherent conservatism of the banking industry in terms of its investments in information technology. "Rip-and-replace" will almost always lose out to "add another layer with a new technology" when it comes to banks' investment in IT, and not just because of the cost factor: there are also considerable risks associated with rip-and-replace security. Secondly, there is the present state of many banks, where financial constraints make sweating existing assets the order of the day.

Thus we see that online banking is growing as an activity and involving increasing amounts of money and that, as a result, the profile of banks' online channel as a target for organized crime is being raised. Datamonitor's research has also shown

that banks are increasing their IT spending on their Web-based services this year, both in terms of heightened security for online payments and the general development of their online channel.

A number of segments within the IT security industry thus have an opportunity to take advantage of this situation, selling products and/or services into retail banks to help them respond to the challenge that the growth of their internet banking business represents.

There are opportunities in client-side and back-end authentication technologies

Datamonitor has identified opportunities for vendors of multi-factor authentication technologies, using the term in its broader US definition. This is because, for historical reasons, Europe tends to think of two- or multi-factor authentication (2FA/MFA) as the delivery of some piece of technology (such as a token or a one-time password (OTP) generator) into the hands of the account holder, whereas North America understands the phrase to include technologies that banks deploy in their networks to better inform the decision to authorize a request to access an online account, such as IP geo-location or machine identification.

Given the sheer variety of client-side technologies now available for providing an additional authentication factor, there is also an opportunity for consultancy firms and systems integrators that can help banks through this veritable maze of products, explaining the relative strengths and weaknesses of each, how each would integrate with their existing security infrastructure and, where appropriate, helping run an implementation project.

There is also an opportunity in the post-sale after-market for customer training, whether it be helping banks to design programs or actually running them on a bank's behalf.

TECHNOLOGY EVOLUTION

This chapter discusses what constitutes 2FA/MFA and how adoption has progressed in Europe, Asia Pacific and North America. It also discusses the broader understanding of what constitutes 2FA/MFA in the US in relation to Europe, which is the result of the Federal Financial Institutions Examination Council's (FFIEC) non-prescriptive approach to technology. This section also points to how mobile phones are gaining ground as a means of delivering an OTP and obviating the need, for instance, for hardware tokens.

Adoption of 2FA/MFA has varied markedly by region

Internet banking made its debut in most developed world countries in the 1990s, although Germany had been using TAN lists (see Definitions section for more information) to enable the remote authorization of transactions for a much longer period.

In the first phase of online services, in most countries a username and password were considered to be adequate protection for any account holder logging in to their online service. There were, however, exceptions: Dutch banks adopted OTP technology as an additional layer of security much earlier than their counterparts in other countries as a result of being hit by a massive phishing attack in the late 1990s that resulted in big losses. Some Nordic countries, and particularly Sweden, followed suit, deploying a mixture of knowledge-based authentication (KBA), public key infrastructure (PKI) and one-time passwords (OTPs).

A username and password are often jointly thought of as the first of two or multiple factors that can be used to authenticate a person's identity for purposes of access to a given website or network, or indeed to authorize a financial transaction carried out online. The classic factors are:

- **Something you are** – such as a person's name or a biometric identifier such as a fingerprint.
- **Something you know** – such as a password, or indeed a mother's maiden name.
- **Something you have** – such as a pass, an ID card or a token.

Since a username and password are together considered to be the first factor for authentication purposes, the 'something you have' element becomes the second in a 2FA system, although such technology is also referred to as strong or multi-factor authentication.

Europe was first to adopt 2FA

European banks actually took the lead in deploying 2FA technology, although the situation was by no means homogeneous across the entire continent. As mentioned above, as long ago as the late 1990s banks in regions such as Benelux, as well as the Nordics and Eastern Europe, began to distribute hardware tokens from companies such as Vasco and RSA to their retail customers for this purpose. These countries were followed by the UK, Italy, Spain and, to some extent, Germany during this decade. France, on the other hand, is only now looking at the adoption of 2FA in response to the publication of a government guideline. In the case of Italy, 2FA has evolved not through legislation, but rather via a cultural evolution, in which the large banks implemented tokens. As those projects matured, the rest of the banks have followed, such that 2FA has become a sort of "me too" requirement for an online bank in Italy.

Some tokens are activated by the user punching in a PIN number, whereupon it generates a OTP that can be input after a username and password to guarantee that the user is who they claim to be. Others do not require the PIN. In either case, these systems mean that, as well as compromising a person's username and password, a fraudster would also have to be in possession of their token in order to carry out an exploit against their account.

Another authentication method that has gained some traction in certain markets such as the UK involves an application using the EMV standard for chip cards. The application is called the Chip Authentication Program (CAP) and was developed by MasterCard, being subsequently adopted by Visa under the name of Dynamic Passcode Authentication (DPA). Therefore, the technology is often referred to as EMV CAP or EMV CAP/DPA.

The CAP specification covers the technical characteristics of a card reader, again often called a CAP reader, with a slot for the chip card, a decimal keypad and a screen capable of displaying up to 12 characters. Bank customers can thus be issued with a CAP reader such that, when they want to access their bank account, they insert their card into the slot, which results in the generation of an OTP that can be used for log in.

There are in fact three different use modes for EMV CAP, with the user able to choose which mode they want to use each time they insert their card into the reader. These are:

- **Identify** – without requiring any further input, the CAP reader interacts with the smartcard to produce a decimal one-time password, which can be used, for example, to log in to a banking website (i.e. the mode described above).
- **Response** – this mode implements challenge-response authentication, where the bank's website asks the customer to enter a 'challenge' number into the CAP reader, and then copy the 'response' number displayed by the CAP reader into the website.
- **Sign** – this mode is an extension of the previous, where not only a random 'challenge' value, but also crucial transaction details such as the transferred value, the currency, and recipient's account number, have to be typed into the CAP reader.

These second and third modes are suitable for use in transaction signing, although the banks that have so far issued CAP readers in the UK, of which the best known is Barclays with its PINsentry device (which it began distributing in 2007), have implemented only the 'identify' and 'sign' modes.

The downside of such an arrangement, and one which has been criticized by competitors both in banking and technology, is that it requires the account holder to carry yet another device with them, along with the wallet holding the card, their mobile phone, laptop, BlackBerry and so on. It is thus also one more device that people could accidentally leave at home when they need it or, worse still, forget on the bus or train. Technology vendors with a software-only offering, based for instance on sending OTPs to mobile phones, can therefore argue that theirs is a more convenient solution, in that most people (at least in the developed world) already carry a phone with them.

Initiatives in Asia Pacific got underway mid-decade

The Asia Pacific region came to additional-factor authentication somewhat later than Europe, but has made some innovative moves since joining the fray. A pioneering institution in this context was New Zealand's ASB Bank, which as long

ago as 2003 announced that it was distributing mobile phone software which enables the mobile to act as an authentication device (the product in question was RSA Mobile).

It was a couple of years later, however, that things really began to take off in the region, with authorities in Hong Kong and Singapore issuing instructions to the banks in their territories to adopt 2FA in 2005, the same year that the Australian Bankers Association announced that its members were all planning to deploy the technology.

Earlier this year, the Commonwealth Bank of Australia (CBA) unveiled plans to expand its NetCode 2FA service from 80,000 customers with high daily transaction rates to all of its 2.5 million online banking customers.

Of course, with experience has come an awareness of the shortcomings of a strategy that depends exclusively on 2FA. As long ago as November 2006, the then group security strategist for National Australia Bank was warning bankers at a conference in Singapore to go beyond authentication, gathering data at all levels with technologies such as intrusion detection/prevention, and to “correlate data from multiple channels and sources.”

Equally, after issuing its first diktat on 2FA in 2005, this month the Hong Kong Monetary Authority told banks to further strengthen their online security infrastructure after it detected criminals using Trojans to steal banking customers' OTPs, resulting in three operations this year in which funds were transferred to bogus accounts.

In the US, the FFIEC called for the implementation of 2FA, but was not prescriptive about the type of technology

While the US came to 2FA later, it did so by government edict rather than the initiative of individual banks and thus moved with force when it did finally adopt the practice.

Having initially given its opinion on matters of authentication as a means of risk mitigation and management for online banking services in 2001, in October 2005 the FFIEC (an interagency government body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by their respective regulators) updated its guidance for “Authentication in an Internet Banking Environment”.

The US has a broader definition of 2FA/MFA than Europe

This is where the common perceptions of what constitutes 2FA or MFA in Europe and the US begin to diverge. As already mentioned, by the time of the FFIEC's second round of guidance in 2005, Europe was already quite a long way down the road of 2FA based on physical tokens, TAN sheets or scratch cards distributed to bank account holders, so much so that such systems are often thought of as synonymous with 2FA.

The FFIEC, on the other hand, called upon all US banks (which run to some 10,000 institutions) to deploy 2FA by the end of 2006, but was not prescriptive about what form this technology should take. In other words, it would be acceptable for a bank to choose to deploy technology that checked for another authentication factor in a different way, without resorting to placing a token or OTP generator in the hands of the account holder.

The FFIEC's non-prescriptive approach has spawned alternative technologies in the US

Considering the cost involved in acquiring, distributing and supporting hardware tokens, many US banks restricted such technology to their corporate/business banking businesses, opting for other forms of adding an extra factor for their retail banking. Many of these extra factors entailed the deployment of some form of technology in their own network that can provide additional information on the person (or at least the machine) trying to log on for purposes of authentication, rather than distributing devices to their customers.

Thus, in response to the FFIEC requirement, US banks have deployed a range of technologies to provide a second factor, including machine authentication and behavioral analysis. If someone tries to log on from an IP address or a machine that is not normally associated with them, or at a time of day when they have never before done any internet banking, these technologies are designed to trigger an alert upon which the bank can then decide whether to make, say, a call to the customer's mobile phone, to check that they are indeed seeking to access their account online or to transfer a given amount, and so on.

This has also resulted in the emergence of a whole range of companies offering technologies to analyze traffic, IP addresses, information about the machine requesting access, and so on, which avoid any additional technology being distributed to account holders, instead sitting in the bank's network.

Mobile phones are gaining traction as a channel for delivering a second factor

Also popular, particularly among smaller institutions, are low-maintenance technologies to substitute hardware tokens, such as software tokens or image recognition as a form of password (see the description of PassFaces' product). A cheaper alternative to hardware tokens is to send OTPs to a phone via SMS. Some banks such as CBA have opted for hardware-based authentication for the customers from which they generate the most revenue, while using SMS OTPs for the rest. There are a number of companies globally developing some form of phone-based authentication, targeting Tier-2 and -3 institutions such as credit unions in the US, as well as institutions in Asia Pacific.

Surveying the global scene, Datamonitor sees that banks have now deployed a plethora of different mechanisms to increase log-in security, including random prompting of digits, virtual keyboards, code sheets. In recent years there have been some high-profile examples of banks starting to issue cards to their account holders to generate OTPs. However, Datamonitor expects such cases to be the exception rather than the norm, and predicts that lighter-touch alternatives, whether in the form of software tokens sent to mobile phones or network-based second factors like PassFaces', to enjoy broader appeal thanks to the lower cost of ownership for the bank.

CUSTOMER IMPACT

Enterprise IT security is often compared, in terms of a target for companies' capital expenditure, with insurance for private individuals. The analogy is that insurance is a worthy investment but not one that delivers immediate or tangible returns, relying as it does on the insured person having an accident, being robbed or dying for it to come into its own.

By the same logic, information security only reveals its value when someone tries to hack into a company's mission-critical data, until which time the money might be better spent on R&D or more marketing initiatives.

Online security must be integral to banks' business

For banks, however, that argument clearly does not hold water, since their very reputation is built on the security with which they hold other people's money. Investment in increased security for their online banking service is thus an essential part of their business. Among other things, it will enable banks to avoid:

- financial loss;
- reputation damage;
- fraudulent data;
- unenforceable or unbinding legal documents and contracts.

Furthermore, banks seek to drive an increasing amount of the day-to-day business that they must carry out, yet which does not generate revenue, to their websites, reserving their branch and personal advisors' time for more valuable activities. It is therefore a key part of that strategy that their internet service is known to be secure.

While the tiered security approach mentioned above can be seen as a practical way of restricting capex on the most expensive technologies to only the most valuable customers, banks could also make a virtue of necessity by advertising their 'platinum' security offering for top customers as part of an aspirational level of banking relationship.

A tiered approach to online security is advisable

Given the range of technologies now on offer and the significant variety already in use around the globe, not to mention the huge cost involved in acquiring and supporting some of them, an overriding conclusion is that banks should adopt a tiered approach to online security and that, as a result, vendors should advocate such a strategy. As the technologies range in cost and security offered, and as the correlation between high cost and high security is not always a direct one (i.e. the cost/effectiveness ratio does not always display inverse proportionality), banks will weigh their alternatives carefully in seeking to heighten their online security.

The most rational answer is to give account holders who do not generate large revenues for banks (because they do not keep a lot of money in their accounts) some form of basic 2FA, complemented by something like machine identification or IP geolocation (see section on Quova in Competitive Landscape and Definitions for more details). Meanwhile, mass affluents, frequent travelers and high net worth individuals should be furnished with correspondingly higher levels of security infrastructure, all the way up to hardware tokens for the most valuable customers.

As phishing increases banks will need to do more on reverse authentication

So far this report has only discussed the scenario in which a bank's customers need to authenticate themselves to the bank in order to log in to their internet service or carry out a transaction involving a fund transfer. However, there is a relatively new requirement in authentication now emerging—reverse authentication. This is where the bank needs to authenticate itself to the customer. The driver here is the increasing number of exploits based on phone calls, emails or even web redirects in which the customer thinks that they are interacting with the bank, when in fact they have fallen into the hands of fraudsters.

With a growing number of banks deploying some form of 2FA and a good proportion of them relying on some form of 'something you know' such as a OTP on the account holder side, it is logical that fraudsters should attempt to intercept credentials via some form of MITM attack.

For instance, if someone seeking to log in to their internet banking service can be redirected to a bogus website that looks very much like their regular internet bank, or if fraudsters can convince the account holder via an official-looking email to disclose their credentials, they can access the account and withdraw funds. Even with a specific OTP generated for a particular internet banking session, if they can discover the OTP and are quick enough to exploit it before the session has finished, they can still do their damage.

For this reason, a number of banks have begun to adopt a strategy of reverse authentication, whereby they can prove to the customer that they are indeed interacting with their bank, whether on the Web, by phone, or via any other channel.

Such technology will need to become more prevalent as the online space becomes an increasingly important attack vector. If banks fail to take up these technologies, they risk customers abandoning online due to a lack of confidence, with a corresponding increase in costs if these customers return to the branch to make basic transactions.

User education will be required for some types of technology

Depending on the type of technology that banks adopt for this additional security, there may be a requirement for user education regarding how it works and what to do if it does not work. While a non-functioning hardware token will usually require a call to a helpdesk, there are scenarios for which the user should be trained; for example, if a user expects a particular image to appear on a web page prior to logging in and that image does not appear they should know not to log in.

COMPETITIVE LANDSCAPE

There are literally hundreds of companies developing one type of technology or another to provide additional security for online banking, and it would be impossible to mention them all. What follows is a list of a few of them, some because they are particularly representative of the kinds of technology under development, and others because Datamonitor found them interesting.

For purposes of rough categorization, they are separated into two groups. First there are those who are working on technologies that are designed to find their way into the hands of the account holder (what are elsewhere referred to as client-side technologies), or that at least are “customer facing” in the sense that the account holder is aware of their existence. Then there are those whose technology is destined to be transparent to the banking customer, sitting as it does in the bank’s network, or in some cases in a third party service provider’s infrastructure, and analyzing some aspect of an online banking session.

The categorization is blatantly flawed, as most of the companies that started life out on the client side are moving into the network with complementary technologies such as behavioral analysis, either developing them themselves or acquiring companies that have done the job for them. This is why major authentication server and token vendors such as RSA and Entrust appear in the second list rather than the first. Equally included in the first are vendors of new types of 2FA technology that does not entail the distribution of any physical device to the account holder.

Nonetheless, the categorization does serve to at least point out that there are these two broad areas of technology which, if anything, are destined to collaborate and complement each other, rather than compete for the same corporate budget.

Client-side technologies

ActivIdentity

ActivIdentity is an authentication server vendor with business in three market segments: business-to-employees, business-to-customer and government-to-citizen, though it sees a trend towards the convergence of the first two. In other words, it believes banks and other enterprises want to leverage their investment in the same authentication server for both their employees and the customer/consumer.

It currently has two separate product lines, 4Tress Authentication Server and 4Tress AAA Server, the former for the financial sector and the latter for general remote access requirements in enterprises, but the plan, as a result of its perception of where the market is going, is to converge the two over the next year.

ActivIdentity casts itself in the “versatile” authentication server segment and preaches “adaptive” authentication, whereby the strength of the authentication method is determined on the fly by real-time scoring.

In other words, it takes into account the initial security posture of the machine from which the user is logging in (how up to date is its anti-virus software, for instance), geolocation, whether it is the user’s own or a corporate PC and a number of other factors including their recent access history to determine whether they score high enough to trigger an additional challenge such as a further security question.

Authenticate

Given that any authentication technology that uses the internet to deliver the extra factor in 2FA/MFA is susceptible to MITM/MITB attacks, it is to be expected that there is now a lot of talk about the need for out-of-band authentication (OOBA), with the preferred second channel usually being the phone. While most vendors have gone for an OTP forwarded to a cellphone via SMS, however, Authenticate uses traditional interactive voice response (IVR) telephony to achieve that factor.

The idea is that a bank determines a point during an online banking session when the account holder should receive an automated phone call, which will typically be when they are about to transfer a significant sum of money. The call will say: "You are requesting a transfer of \$XXX to the account ending in '1234'. If this is correct, please press 1 to confirm."

Thus if an MITB attack has intercepted the transaction, added another \$5,000 and changed the destination account, the user can nip the exploit in the bud. Authenticate does also offer SMS messages as an alternative, but admits that it prefers the voice because it is a closed loop.

There is also an enhanced version of the service which it refers to as offering a third authentication factor, in which an account holder signing up for the service records their voice and then, whenever they are being authenticated, Authenticate compares the voice on the current call with the recorded one, using technology from speech recognition specialist Nuance.

Authenticate was founded in 1999 and has, from the outset, adopted a software-as-a-service model, charging its customers an initial fee to set them up, plus a per transaction fee thereafter. It markets itself directly, but also through distribution partners RSA and VeriSign.

Commerce Media

Commerce Media offers a 2FA system that uses an out-of-band means of delivering the second factor. The principal one is an SMS sent to a mobile phone, but it can equally well be via email.

The UK company's product is called Celo and it considers one of its differentiators the fact that it is already ISO 27001 compliant and is approved for use on List X, i.e. the list of sites on which UK government protectively marked information can be displayed, which are mainly sites involved with defense research and manufacturing that is vital to national security.

CRYPTOCARD

CRYPTOCARD is a player in the authentication market with its CRYPTO-Server product and the AuthEngine set of programming objects and APIs for integration with customers' applications. It has also begun offering authentication as a Cloud-based service called CRYPTO-MAS.

CRYPTOCARD also offers a line of tokens, though like most players these days it support multiple other vendors' tokens, whether through their API or a standard such as OATH. It has recently unveiled a partnership with secure USB stick vendor IronKey whereby it ships its authentication technology on an IronKey fob and has entered the market for card-based OTP generators via an agreement with Swiss manufacturer NagraID and Australian developer Emue Technologies.

Fronde Anywhere

Fronde Anywhere is a New Zealand-based software developer that offers banks an application to reside on account holders' mobile phones and generate OTPs for logging onto their internet bank. The application, called TwoSecure, can generate three flavors of OTP, namely a Standard OTP, a Challenge Response OTP or a Transaction Signed OTP, for different levels of security requirement.

Gemalto

The French smart card heavyweight is the result of the 2005 merger of Gemplus and Axalto. While best known for its smart card acumen (it has some 800 million of its card in circulation around the world), Gemalto in fact has a full range of authentication products, from the server through to credentials in multiple form factors, including soft tokens for mobile phones and USB sticks.

On the consumer authentication side into which online banking falls, its Ezio portfolio offers its unconnected technology (based on mobile phones, classic OTP generating tokens and smart cards), while for enterprise authentication it has a connected offering, which consists of card readers and USB sticks that plug into the user's PC.

GrIDsure

UK-based GrIDsure is one of a number of companies that have developed technology to provide an additional authentication factor for people logging on remotely. Its offering is a grid, four boxes by four, in which a person selects four contiguous boxes to form a pattern such that, whenever presented with a grid in future, they will be able to repeat that shape, regardless of the numbers that are in the individual boxes. Thus by randomizing the numbers in the boxes, the four-number code generated each time is different, the person logging in only having to remember the shape they have chosen.

The grid can be presented on the same machine on which the person wishes to log onto their internet bank, but can also be presented on a mobile phone with the person inputting the numbers on the computer.

There is also a low-tech version for developing countries, can be distributed on a printed card with numbers that slide through a grid printed on an outside sleeve, in which case it can be used for phone banking: a call center operative can instruct the account holder to move the inside card to, say, the fifth position as shown by a number along the top, then read out the four numbers that are showing in the holes he or she has made in the grid corresponding to the chosen shape.

Returning to the online banking scenario, GrIDsure says that, if a hacker seeks to steal the numbers corresponding to the account holder's chosen shape during a particular session, they might try doing a screen shot, but since GrIDsure's screens are only bit maps, the HTML won't. It would therefore need an OCR to interpret the graphic, plus a key logger, and would need to be done three times in order for the hacker to reverse engineer the information, all of which would require a fairly hefty Trojan to be planted on the machine.

There are also techniques for a further level of security, such as associating the process with a soft keypad displayed prior to the grid, which will befuddle a screen grabber since they are usually event-based and so won't know when to do the grab. The grid can also be associated with a soft token resident on a phone, such that there are no SMS fees.

Gridsure also offers its technology for reverse authentication, whereby a bank could send an account holder a code, be it in a letter or an SMS message, which he or she would type in on the computer to bring up a grid, then the bank could tell the person on the phone which four numbers on the grid showing on their screen corresponded to their chosen shape.

The company refers to these shapes as personal identification patterns (PIPs) and is currently developing a rules-based strength calculator, which will be able to show the account holder at the moment they choose their pattern difficult it is to spoof, with color ratings of red, yellow and green. Gridsure has also worked on a “speaking grid” version for the blind, where it leverages their extra-strong spatial awareness to call out the positions of the boxes.

IBM

Aware that 2FA systems are frequently susceptible for man-in-the-middle (MITM) and man-in-the-browser (MITB) attacks, whereby a criminal inserts code between the account holder and the bank to intercept password, PIN and even OTP information in mid-session, several companies have done research into ways to circumvent MITM. IBM, for instance, launched a product last year called Zone Trusted Information Channel (ZTIC), consisting of a USB stick with a dot matrix display and minimal I/O capabilities. It runs the full TLS/SSL encryption protocol and starts a “pass-through” proxy that is configured to connect with pre-configured banking websites.

After starting the ZTIC proxy, the user opens a Web browser to establish a connection with the bank’s Website via the ZTIC. From that moment on, all data transmitted between browser and server pass through the ZTIC; the SSL session is protected by keys maintained only on the ZTIC and, hence, is inaccessible to malware on the PC.

Furthermore, all critical transaction information, such as target account numbers, is automatically detected in the data stream between browser and ZTIC. This critical information is then displayed on the ZTIC for explicit user confirmation: Only after pressing the “OK” button does the TLS/SSL connection continue. If any malware on the PC has inserted incorrect transaction data into the browser, it can be detected by the user at this moment.

IBM has also created versions of ZTIC with further layers of security, such as on that comes with client-side keys embedded in the USB stick and require a card to be plugged into ZTIC to authenticate it for use.

PassFaces

Although founded in the UK in 2000, PassFaces is today headquartered in the US, its founders having almost immediately determined that the principal market for its technology was on that side of the Atlantic, not least because many European banks were already established users of token technology.

Its move to the US actually pre-dated the FFIEC guidelines, but this development clearly put an extra wind into its sails, as Tier-2 and -3 institutions suddenly faced an impending requirement to offer some form of online security beyond user name and password.

Its offering is as follows: PassFaces built a database of photographs of people which form the basis of its technology. A bank buys its photo library, then when an account holder signs up for online banking, they are allocated, at random, three of the myriad of faces as a kind of “image password”. Every time they then want to log on, they are presented with three successive grids of nine photos, each of which contains one of their three faces. They click on the appropriate photo in each grid, and are granted access.

The system is sold as a library of faces plus the application that presents them to the account holder, and PassFaces says its sweet spot tends to be in smaller banks (its largest deployment in the financial sector is in a credit union with 35,000 users), who obviously are attracted by the absence of tokens or anything else that needs to be distributed to account holders and managed remotely.

SafeNet

While it is perhaps best known for its encryption technology, not least because it sells into major US government agencies, SafeNet is expanding its horizons since its merger, in January this year, with Israeli security vendor Aladdin Knowledge Systems. It now has four sectors, which are its traditional hardware security modules and data protection, plus software rights management and authentication.

In the authentication market, it currently has three product lines:

- the iKey USB token and smart card portfolio which comes from SafeNet itself,
- the eToken line from Aladdin and
- SafeWord, an OTP generation technology Aladdin acquired last year from Secure Computing, so there is certain to be some sort of rationalization of these lines, though clearly SafeNet will need to tread carefully if it is to retain customers. It sees, in addition, the future requiring it to offer soft tokens and technology on mobile devices for authentication purposes.

It clearly also wants to make its authentication server as heterogeneous as possible, not only covering the disparate token technologies it now has in house, but also to include technologies from other companies. It is not, however, currently planning to support all OATH-compliant devices, but rather to integrate with partners' technology through their APIs.

SecurEnvoy

SecurEnvoy was founded in 2000 to develop two-factor authentication that does not require tokens, its flagship product being SecurAccess, which uses the mobile phone as the channel through which to deliver the additional factor. The system works by SecurEnvoy pre-sending a user's first access code to their phone before they need it because it considers reliance on a real-time capability as inherently flawed.

The code has an active life which is timed from the moment the account holder begins to use it and is automatically replaced by SecurEnvoy when it comes to the end of its validity. There is never more than one code on the phone at any one time, the company guarantees.

SecurEnvoy offers its technology as licensed software or in a managed service model. It has recently added features for mass market, B2C implementations such as self-enrollment and self-management. SecurAccess has also been "decoupled" from ActiveDirectory, to which it has long integrated for enterprise deployment purposes, but in the latest version it sits as a separate directory and so overcomes the issue of additional AD licenses in very large deployments such as B2C environments.

Thales

Thales is a major French engineering conglomerate with activities in aerospace, defense, transportation and security. It got into the authentication business in 2004 with the launch of its SafeSign Authentication Server, its strategy for which, given that it was entering a market already inhabited by major players such as RSA and Vasco, was to debut supporting any form of credential from the outset (tokens, SMS OTP and EMV CAP, for instance).

This flexibility enabled it to offer its product into heterogeneous environments where, for instance, a company might use EMV CAP for retail, proprietary smart cards for corporate banking and tokens for its mobile workers, whereas some of the industry's big guns still only support their own tokens on their authentication servers. On the token side, SafeSign supports all OATH-compliant devices, as well as proprietary ones from Vasco and ActivIdentity.

Thales told Datamonitor that RSA had declined to open up its technology for SafeSign to support its SecurID tokens, so instead it uses the Security Assertion Markup Language (SAML), an XML-based standard for exchanging authentication and authorization data between security domains, to enable a session to go back to an RSA Authentication Manager.

Thales does offer its own tokens, but they are more expensive than market leaders such as RSA and Vasco, with more sophisticated functionality and targeted at the corporate banking and treasury functions within a bank.

Vasco

Vasco is a leading player in the authentication market with its Vacman platform and its Digipass portfolio of hard- and software tokens and readers.

As well as the Vacman Controller authentication engine that is linked to online banking applications through an API, the company also offers a standalone authentication server called Identiskey, which is a software-only product based on the Vacman authentication engine, and an appliance version called aXsGuard Identifier, which is targeted at smaller banks.

Financial services makes up the vast majority of its revenue and, though it is headquartered in the US, Vasco's largest region for sales is EMEA. Unsurprisingly in the current economic climate, its primary focus for expanding its business this year is in Southeast Asia and the BRIC countries, though it does have an alliance with US core banking system vendor Fiserv for the North American market.

VeriSign

VeriSign's approach to 2FA is to offer it as a service delivered from the Cloud as part of its VeriSign Identity Protection (VIP) suite of services. Its argument for the service approach is a compelling one, in that a bank or other online business joins a network of companies called the VIP Network, all of whose websites can accept what is called a VIP Credential, such that users can access any of a number of sites, including their bank's, rather than having to carry around a bevy of different tokens, one for each service.

VIP Authentication supports all open standards, OATH-compliant form factors for the customer device, which comprises a wide range of credential types (OTP security cards, OTP tokens, OTP Flash drives, SMS OTP, voice-enabled passcodes, browser toolbar OTPs, PKI certificates and, most recently, mobile phone credentials). The only one of these VeriSign actually produces is the OTP generator for mobile phones, which it makes available for free download, with versions for the

iPhone and for all handsets that support Java. In all other cases, the devices are from third parties, i.e. any manufacturer that supports the OATH standard.

VeriSign monetizes the service by charging credential issuers an annual fee for the validation service while so-called relying parties pay a separate fee for it to validate people coming onto their site. While many consumers will likely be issued some form of VIP Credential from their bank (in which case the credential will be co-branded), they can also purchase one directly from VeriSign on a self-service portal called VeriSign Identity Protection Center.

Vett

A small UK start-up is currently evangelizing about a technology it positions as multi-factor authentication for remote (i.e. not face-to-face) transactions. In an online banking scenario, a fund transfer would work as follows:

- 1) An account holder would connect to their online banking facility and select the option for fund transfer. They would then enter the details of the payee, their customer reference number (if the payee is a utility) and the amount to be transferred.
- 2) The bank would forward a copy of the customer's instruction to their registered email address, or to their mobile phone via SMS. This communication contains a unique reference number for the transaction.
- 3) A duplicate copy is sent to Vett.
- 4) The customer connects to their bank to be authenticated.
- 5) Vett requests input for the unique reference number, locates the customer's instruction and reports the details. Once the system has received the customer's authorization, their account is checked for the funds. The bank then flags the amount to be paid and debits the account accordingly.
- 6) A payment message is generated and the funds are directed to the payee's account.

Vett argues that its system has the advantage of working with a bank's existing security infrastructure, as well as giving the customer the opportunity to review the transaction prior to confirming. It should also minimize repudiation, defeat phishing attacks and, it argues, extend online functionality.

Back-end technologies

ACI

ACI Worldwide is best known for its electronic payments software, but since last year it has been offering a real-time online banking fraud prevention service through a partnership with Australian security developer Eunexus.

In essence, the partnership brings together Eunexus' IP profiling technology, which goes from basic IP address inspection to a more in-depth analysis based on a database of confirmed sources of fraudulent activity, with ACI's real-time transaction monitoring capability, called Proactive Risk Manager.

The ACI product has in fact been around for a decade or so, having debuted in the credit card market and then subsequently been taken multichannel about five years ago. It was in 2008 that it gained real-time capabilities, which is a key feature with initiatives such as the UK's Faster Payments being introduced in various countries.

Entrust

Entrust started out on the authentication server and token side of the industry, where it continues to do a lot of business, but has also expanded into fraud detection through behavioral analysis and so-called velocity checking (i.e. seeing how often a credit is used on a particular site or an individual is making transfers from a particular bank account) with its TransactionGuard software.

TransactionGuard checks all user activity around HTTP-based transactions and is designed to provide centralized fraud intelligence. As on-premise software rather than a service delivered from within the Cloud, it can be thought of as competing with RSA's PassMark technology, though of course the Cyota service from RSA is also competing for banks' budget.

On the authentication side, meanwhile, Entrust plans to expand its support for credentials from third parties such as PassFaces, which it will do through the OATH standard later this year.

Ericsson

The Swedish telecoms equipment vendor is not a name one typically associates with enterprise technology generally, let alone with security for online banking, but a business units within the group called IPX is now entering precisely that market.

IPX was set up in 2001 to operate as a broker between content providers and mobile operators to enable the former's product to be sold through the latter's channel and handle the payment process. It then expanded into bulk messaging, buying SMS capacity from operators and reselling it to enterprises such as hospitals and airlines, and now it seeks to broker other assets from mobile operators, namely country location information.

The granularity of the information it will be able to provide is not high. It will be able to tell a bank which country someone is in when they are logging onto their internet banking site, provided they have switched their mobile phone on since arriving in the particular country.

More specific location will depend on the country, since the mobile operators in some countries allow it to cull cell ID information, while in others they do not. The technology is also specific to the GSM world (i.e. it doesn't work with CDMA phones, which are a major part of the North American market, as well as Korea and Latin America), but then GSM is at least ten times the size of the CDMA market worldwide.

Guardian Analytics

Guardian Analytics is, as its name suggests, a company that develops technology to monitor multiple aspects of an online banking session (machine ID, network operator, what is installed on the machine, the time of day and day of the week, the types of activity undertaken) in what it terms "dynamic account modeling" so as to build a predictive model for each of a bank's online customers.

It deploys its technology as software that sits on the bank's premises, with one instance placed alongside each online application in order to monitor all the aspects mentioned, then feed them into its risk scoring engine which will then inform an authentication server to grant the person access or generate an alert to a risk application. In addition to collecting data for the individual customer, it also does correlations across a bank's customer base to see whether an exploit is underway and attacking multiple users.

The audience for the technology is, of course, a bank's fraud prevention team, its risk management team and audit and compliance officers, all of whom are provided with a Web GUI with which to view Guardian Analytics' results.

lovation

lovation is a company set up in 2004 to create what it calls a "device reputation authority", which means that it has a database with information on over 100 million desk- and laptop computers, relating to which bank accounts they connect to and any problems relating to that machine such as whether it has been a source of malware. It counts banks, online gaming, gambling and internet dating sites among its customers and delivers its technology as a service.

lovation's customers select what it calls key interaction points at which to check on a machine's reputation, such as, in the case of a bank, during account creation, when a deposit or withdrawal is being made, or when someone is making an application for credit. It refers to the process whereby it develops a usage and security profile for an individual machine as "deviceprinting" and while the account holder's identity is information that stays with the bank, lovation compiles the information on the device from which the person is logging in.

While lovation's technology is transparent to the people trying to log onto any of its customers' sites, it requires its customers to warn these people (e.g. a bank must warn its customers) that their machines are being profiled by the service. It places a small piece of encrypted data resident on a machine that has been "deviceprinted" which it seeks when any future online session with one of its customers is being initiated. The company says that it is currently adding another five million devices to its database each month and, for the last year or so, less than 1% of the machines it is analyzing do not have the encrypted data on them.

The only thing the bank needs to provide to lovation needs from the bank is the account number, which can then be associated to a particular machine's identity, such that if the same account holder later logs on from another machine, that information too will be recorded so that the bank can build up a profile of the person's most commonly used machines. lovation also builds up relational maps between machines, which may show, for instance, that a husband and wife will both log on to the same account from different machines. If there is a problem with the account, lovation can provide intelligence on what other websites have been access from that machine to see whether they were infected, for instance.

The company considers its value proposition to be fourfold:

Firstly, there is the intrinsic value of seeing traffic down to the individual machine, which means that if 50 accounts have been created in a single day from the same machine, it is a sure sign that something strange is going on.

Secondly, lovation is a useful adjunct to any other risk mitigation technology a bank may have in place such as a risk scoring service on credit card transactions.

Thirdly, in the area of online sex offenders, the service can put a stop to the so-called revolving door syndrome, whereby a criminal who is detected on the log of a particular chat room logs off and tries to log on to another.

Finally, there is the network effect by which one customer can benefit from information gathered on a particular machine when it was logged on to another site, which may not even be in the same area of business.

Quova

Currently the doyen of geolocation information is Quova, a US company with customers in the financial sector in various geographies, including Europe. Quova provides IP geolocation, and a lot of its business in North America is in online gambling, since US citizens are not allowed to take part in such activity.

European banks, on the other hand, have seized on the opportunity to identify where someone is logging in from and to use that information to assess the risk in authorizing access to a given bank account.

Quova does sell directly, but it counts on major partners such as RSA (the former Cyota business), VeriSign and Oracle to penetrate major accounts. It also offers an add-on for wireless connectivity via a partnership with US developer Mexens, whose Navizon product enables it to locate where a laptop is by referencing the access point to which it is attaching.

RSA

RSA, which since its acquisition in 2006 has been the security division of storage heavyweight EMC, is a major player in the authentication market with both server and token technology.

However, it has also been active in developing a business in what it calls risk-based authentication (RBA) services, whereby it profiles devices and user behavior (the normal geography from which a person logs onto a website, their preferred time of day, etc.,,) and collates that information with data from RSA's eFraudNetwork, which it describes as "the industry's first and largest cross-institution, cross-platform online fraud network dedicated to sharing and disseminating information on fraudulent activity."

It built its RBA offering through two acquisitions, namely Cyota and PassMark, which essentially did the same thing but the first delivered it as a service, the second with on-premise technology, enabling RSA to adopt a deployment-agnostic stance.

The decision to get into RBA was undoubtedly motivated, at least in part, by the FFIEC's guidance for US banks, which suddenly faced a deadline to deploy 2FA/MFA and sought ways of complying without a massive capex outlay and without disruption to their customers' online activities. It also sold RBA into some of the companies that deliver core banking systems as a service in the US, again so that their customers could comply with the FFIEC's requirement.

Like location, RSA puts something on the machines being profiled, in its case a cookie, though it is aware that some users delete the cookie, and for them it has another solution in the form of Flash share objects. If they too are deleted, it falls back on what it calls statistical device identity, looking at things like the operating system it is running, what browser, its screen resolution, what language and so on, to come with a "good enough" profile to enable a unique picture of a particular machine.

To date, RSA's RBA offering has been used to generate so-called step-up authentication, such as an additional challenge from the bank to confirm that someone logging on really is who they claim to be. Now, however, the company is moving into transaction monitoring, whereby instead of step-up authentication it can log a transaction and report it to a case management team, who can then analyze it. This is a capability that was already in the Cyota side of the business but has now been transferred across into the PassMark side too.

Tier-3

Australian IT security developer Tier-3 says its Huntsman behavioral analysis software is in use in a major bank in its homeland to complement client-side authentication technologies.

The bank was already using the product on its internal network and so, in essence, the challenge was to deploy it facing inbound traffic from the internet, which meant analyzing a huge volume of data from both a Web portal and from the bank's mainframe in order to derive intelligence about external requests for access and the sessions that they generate.

In addition to collecting data and analyzing it, Huntsman is also programmed to respond, which can vary from a challenge to a user for an additional response to a full-blown cessation of the session.

GO TO MARKET

With internet banking on the increase, in terms of both the number of people using it and the variety of transactions being carried out, selling additional security functionality to banks to support it should be relatively easy. Indeed, as fraudsters increase their focus on the online channel as a source of illicit earnings, demand for security technology from banks is growing.

On the other hand, there are numerous technology options to choose from, so vendors must demonstrate that they are the cheapest in terms of total cost of ownership or the most secure, or that their product sits at the most satisfactory point on the continuum that runs between these two extremes. And of course, since the most expensive solution is not always the most secure, if vendors can show that their technology is highly secure without requiring a huge upfront outlay, so much the better.

Recommend a mixture of technologies

Datamonitor believes that some of the non-client-based technologies that US banks have deployed as a means of meeting the FFIEC's requirements with the minimum outlay are valid, in a wider context and in other geographies, as complementary technologies, rather than as substitutes for tokens, digital signatures and so on.

This fits neatly into the broader approach of advocating a tiered strategy for online security. Technologies such as behavioral analysis, machine identification and IP geo-location could thus be the bedrock layer(s) that are applied to all requests for access, with the more expensive (not to mention intrusive) ones that require the account holders themselves to take some action layered on top for different categories of customer.

Disruption to existing infrastructure is to be discouraged

There is also the issue of how disruptive another layer of security will be to a company's existing infrastructure. If a vendor can demonstrate that its product can slot into a bank's existing systems without the need for the wholesale re-architecting of what is already in place, it will be listened to with greater enthusiasm. The vendor will win further brownie points if the incoming product requires minimal user education.

Banks will need help with user education

If the new technology unavoidably requires a degree of training for the account holders, the vendor should be prepared to shoulder part of the cost of that training program or provide help in delivering it, perhaps with a templated website for the purpose.

Delivering technology as a service will appeal to smaller US and German institutions

Wherever possible, technology vendors should be prepared to offer the option of delivering their product to banks as a service rather than as a product sale, particularly if it has no hardware component. While tier 1 banks have the deep pockets required to countenance a major capex investment on additional online security, smaller institutions will probably already take at least some of their infrastructure as a service.

This is particularly the case in markets with large numbers of banks, such as the US (some 10,000 institutions) and Germany (around 800), in which the concept of the service bureau as a source of technology-as-a-service is well established.

Channel partners will be key in such accounts

Vendors that plan to pursue this business model and target the tier 2 and 3 organizations should also develop solid relationships with resellers, systems integrators and/or service providers. In some cases, a company that is already a reseller in the general enterprise market may be developing a capability to deliver the technology as a service in order to increase recurring revenues and cement relations with its customers, and this will be particularly appropriate for serving smaller financial service institutions.

Since smaller banks and credit unions are more open to outsourcing part of their activities (particularly when they do not think that keeping the activity in-house will add significant value for their customers), they may not have extensive skills in-house in these areas and will thus rely more heavily on a channel partner to deliver the service with, for example, a service level agreement.

Countries with greater banking concentration prefer to buy products

The service-based delivery of technology is less accepted in countries where there is a large degree of concentration in the financial sector, which is the case in the four of the big five European economies (France, the UK, Italy and Spain), as well as in Australia, New Zealand and Japan.

The retail banking market in all of these countries is characterized by the dominance of a handful of huge entities with extensive branch networks and large customer bases and, as a result, by banks with a cultural bias towards owning and operating their own infrastructure, be it their core banking systems or their security infrastructure. In these countries, most security technology is delivered as a product, whether licensed software or an invoiced piece of hardware such as a token.

The fight against fraudsters will go on, so a long game may be in order

Finally, it is worth pointing out that while there is clearly a move to increase the security infrastructure surrounding online banking at the moment, it is no land grab with a deadline beyond which the market opportunity will disappear. The arms race between banks and fraudsters will continue, and new technological answers will be required for tomorrow's security threats. As a result, technology vendors may need to play the longer game, becoming embedded in an account with a smaller-value sale on day one, then growing their presence over time through good service and support. This will enable them to upsell to larger deployments of the same technology or more advanced versions down the road.

APPENDIX

Definitions

CAPTCHA

A CAPTCHA or Captcha is a type of challenge-response test used in computing to ensure that the response is not generated by a computer. The process usually involves one computer (a server) asking a user to complete a simple test which the computer is able to generate and grade. Because other computers are unable to solve the CAPTCHA, any user entering a correct solution is presumed to be human. Thus, it is sometimes described as a reverse Turing test, because it is administered by a machine and targeted to a human, in contrast to the standard Turing test that is typically administered by a human and targeted to a machine. A common type of CAPTCHA requires that the user type letters or digits from a distorted image that appears on the screen.

IP geolocation

Geolocation software is used to deduce the geolocation (geographic location) of another party. On the internet, one geolocation approach is to identify the subject party's IP address, then determine what country, organization, and/or user the IP address has been assigned to.

Man-in-the-middle (MITM) attacks

A man-in-the-middle attack (often abbreviated MITM), or bucket-brigade attack, or sometimes Janus attack, is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances (for example, the owner of a public wireless access point can in principle conduct MITM attacks on the users).

Man-in the-browser (MITB) attacks

Man-in-the-Browser (MITB) is a recent form of Internet threat related to Man-in-the-Middle (MITM), is a Trojan that infects a web browser and has the ability to modify pages, modify transaction content or insert additional transactions, all in a completely covert fashion invisible to both the user and host application. A MitB attack will be successful irrespective of whether security mechanisms such as SSL/PKI and/or Two or Three Factor Authentication solutions are in place. The only way to counter a MitB attack is by utilising Transaction Verification.

One of the most effective methods in combating a MITB attack is through an Out-of-Band (OOB) transaction verification process. This overcomes the MitB Trojan by verifying the transaction details, as received by the host (bank), to the user (customer) over a channel other than the browser; typically an automated telephone call. OOB Transaction Verification is ideal for mass market use since it leverages devices already in the public domain (e.g. Landline, Cell Phone, etc) and requires no additional hardware devices yet enables Three Factor Authentication (utilizing Voice Biometrics), Transaction Signing (to non-repudiation level) and Transaction Verification.

One-time password (OTP)

The purpose of a one-time password (OTP) is to make it more difficult to gain unauthorized access to restricted resources, like a computer account. Traditionally static passwords can more easily be accessed by an unauthorized intruder given enough attempts and time. By constantly altering the password, as is done with a one-time password, this risk can be greatly reduced.

There are basically five types of one-time passwords:

1. Using a mathematical algorithm to generate a new password based on the previous password
2. Based on time-synchronization between the authentication server and the client providing the password
3. Using a mathematical algorithm, but the new password is based on a challenge (e.g., a random number chosen by the authentication server or transaction details) and a counter instead of being based on the previous password.
4. Using a list of passwords printed on paper.
5. Using portable electronic devices (e.g., mobile phones) as an out-of-band method for transmitting one-time passwords.

Out-of-band authentication (OOBA)

Out-of-Band authentication is the use of two separate networks working simultaneously to authenticate a user. Out-of-Band authentication works well because even if a fraudulent user gains all security credentials to a user's account, a transaction cannot complete without access to the second authentication network.

Transaction Authentication Number (TAN) lists

A Transaction authentication number or TAN is used by some online banking services as a form of single use one-time passwords to authorize financial transactions. TANs are a second layer of security above and beyond the traditional single-password authentication.

TANs are believed to provide additional security because they act as a form of two-factor authentication. Should the physical document or token containing the TANs be stolen, it will be of little use without the password; conversely, if the login data are obtained, no transactions can be performed without a valid TAN.

TAN lists are particularly popular in the German banking industry. They work as follows:

1. The bank creates a set of unique TANs for the user. Typically, there are 50 TANs printed on a list, each six or eight characters long, which is enough to last half a year for a normal user.
2. The user picks up the list from the nearest bank branch (presenting a passport, an ID card or similar document) or is sent the TAN list through the mail.
3. The password (PIN) is mailed separately.

4. To log on to his/her account, the user must enter user name (often the account number) and password (PIN). This may give access to account information but the ability to process transactions is disabled.
5. To perform a transaction, the user enters the request and authorized the transaction by entering an unused TAN. The bank verifies the TAN submitted against the list of TANs they issued to the user. If it is a match, the transaction is processed. If it is not a match, the transaction is rejected.
6. The TAN has now been consumed and will not be recognized for any further transactions.
7. If the TAN list is compromised, the user may cancel it by notifying the bank.

TAN lists are, however, susceptible to phishing if a victim is tricked into providing both their password/PIN and one or several TANs. As a result, the industry developed so-called indexed TANs, or iTANs, which reduce the risk of phishing by having the bank request authorization for a transaction by asking for the TAN that is identified by a specific sequence number (index). Since the index is selected randomly by the bank, an arbitrary TAN acquired by an attacker is usually worthless.

However, iTANs are still susceptible to man-in-the-middle attacks, including ones using cross-site scripting, where the user is tricked into logging on to a bogus website. To address this challenge, the industry came up with a variant of iTANs that adds a Captcha for further security. This method is called iTANplus.

Two-factor authentication/Multi-factor authentication (2FA/MFA)

An authentication factor is a piece of information and process used to authenticate or verify the identity of a person or other entity requesting access under security constraints. Two-factor authentication (2FA) is a system wherein two different factors are used in conjunction to authenticate. Using two factors as opposed to one factor generally delivers a higher level of authentication assurance.

Using more than one factor is sometimes called "strong authentication", however, "strong authentication" and "multi-factor authentication" are fundamentally different processes. Soliciting multiple answers to challenge questions may be considered strong authentication but, unless the process also retrieves 'something you have' or 'something you are', it would not be considered multi-factor. The FFIEC issued supplemental guidance on this subject in August 2006, in which they clarified, "By definition true multifactor authentication requires the use of solutions from two or more of the three categories of factors. Using multiple solutions from the same category ... would not constitute multi-factor authentication."

Methodology

- **Interviews** – discussions with leading banks and technology vendors, conducted specifically for this report.
- **On-going vendor briefings** – Datamonitor conducts interviews with software, hardware, networking and services vendors serving the banking sector on a regular basis.
- **Secondary research** – Other secondary sources of information include company reports and web sites, international organization statistics, national and international industry associations, SEC filings, broker and analyst reports, and business information libraries and databases.

Further reading

Online Banking in the Age of Web 2.0 (Strategic Focus), DMTC2192

Web 2.0 in Online Banking: A Progress Report (Analyst Insight), BFTC2311

Business Trends: North American Retail Banking Technology Spending Strategies 2009 (Customer Focus), DPTC0056,

Business Trends: European Retail Banking Technology Spending Strategies 2009 (Customer Focus), DPTC0024

Ask the analyst

Rik Turner

The Financial Services Technology Knowledge Center Writing team

rturner@datamonitor.com

Datamonitor consulting

We hope that the data and analysis in this brief will help you make informed and imaginative business decisions. If you have further requirements, Datamonitor's consulting team may be able to help you. For more information about Datamonitor's consulting capabilities, please contact us directly at consulting@datamonitor.com.

Disclaimer

All Rights Reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher, Datamonitor plc.

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions and recommendations that Datamonitor delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such Datamonitor can accept no liability whatever for actions taken based on any information that may subsequently prove to be incorrect.